(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 696 36 466 T2** 2007.08.09

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 974 129 B1**
(21) Deutsches Aktenzeichen: **696 36 466.2**
(86) PCT-Aktenzeichen: **PCT/US96/14262**
(96) Europäisches Aktenzeichen: **96 932 173.6**
(87) PCT-Veröffentlichungs-Nr.: **WO 1998/010381**
(86) PCT-Anmeldetag: **04.09.1996**
(87) Veröffentlichungstag der PCT-Anmeldung: **12.03.1998**
(97) Erstveröffentlichung durch das EPA: **26.01.2000**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **16.08.2006**
(47) Veröffentlichungstag im Patentblatt: **09.08.2007**

(51) Int Cl.[8]: ***G07F 7/00*** (2006.01)
G07F 7/10 (2006.01)
G06Q 30/00 (2006.01)

(73) Patentinhaber:
Intertrust Technologies Corp., Sunnyvale, Calif., US

(74) Vertreter:
Schaumburg, Thoenes, Thurn, Landskron, 81679 München

(84) Benannte Vertragsstaaten:
AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(72) Erfinder:
SHEAR, H., Victor, Bethesda, MD 20814, US; VAN WIE, M., David, Eugene, OR 97403, US; WEBER, Robert, Menlo Park, CA 94025, US

(54) Bezeichnung: **TREUHAND INFRASTRUKTUR UNTERSTÜTZUNGSSYSTEME, VERFAHREN UND TECHNIKEN ZUM SICHEREN ELEKTRONISCHEN HANDEL, ELEKTRONISCHE TRANSAKTIONEN, STEUERUNG UND AUTOMATISIERUNG VON HANDELSVERFAHREN, VERTEILTE DATENVERARBEITUNG UND VERWALTEN VON RECHTEN**

Beschreibung

Gebiet der Erfindungen

[0001] Die vorliegenden Erfindungen betreffen allgemein die optimale Nutzbarmachung der Möglichkeiten moderner Rechentechnik und Netzwerktechnik für die Administration und die Unterstützung elektronischer Interaktionen und Konsequenzen und ferner eine sichere Architektur als Grundlage für eine verteilte, vertrauenswürdige Administration für den elektronischen Handel.

[0002] Spezieller betreffen vorliegenden Erfindungen ein „Distributed Commerce Utility" als Grundlage für die Administration und Unterstützung des elektronischen Handels und anderer elektronischer Interaktions- und Beziehungsumgebungen.

[0003] Noch spezieller betreffen die vorliegenden Erfindungen im Allgemeinen folgendes:

- die effiziente Administration und Unterstützung des elektronischen Handels und Datenverkehrs;
- Verfahren und Technologien für elektronische Rechteadministration und Unterstützungsdienste;
- Verfahrensweisen und Anordnungen für die Verteilung von Administrations- und Unterstützungsdiensten wie sicheres elektronisches Transaktionsmanagement/sichere elektronische Transaktionsadministration, elektronische Prozesssteuerung und -automatisierung und Clearingfunktionen zwischen und/oder innerhalb von elektronischen Netzwerken und/oder virtuellen Verteilungsumgebungen; und/oder
- Clearing, Steuerung, Automatisierung und andere administrative, infrastrukturelle Einsatzmöglichkeiten und Unterstützungsmöglichkeiten, die zusammen einen effizienten, sicheren, Peer-to-Peer-basierten Austausch zwischen Geschäftsteilnehmern in der digitalen Gemeinschaft von Personen ermöglichen und unterstützen.

Technischer Hintergrund

[0004] Leistungsfähige und erfolgreiche Gesellschaften benötigen Mittel, mit deren Hilfe ihre Mitglieder die Art und die Konsequenzen ihrer Teilnahme an Interaktionen steuern können. Jede Gemeinschaft benötigt gewisse Basisdienste, Einrichtungen und Anlagen:

- die Post liefert uns die Postsendungen,
- die Schulen unterrichten unsere Kinder,
- das Autobahnamt wartet unsere Straßen und hält sie instand,
- die Feuerwehr löscht Feuer
- die Stadtwerke beliefern unsere Haushalte mit elektrischem Strom,
- der Telefonanbieter verbindet überall Menschen und elektronische Geräte untereinander und stellt Auskunftsdienste für jene bereit, die die Nummer nicht wissen,
- Banken bewahren Ihr Geld sicher auf
- Kabelfernseh- und Rundfunkanstalten übertragen Nachrichten- und Unterhaltungssendungen in die Haushalte
- die Polizei sorgt für Ordnung,
- die Stadtreinigung entsorgt den Müll und
- Sozialeinrichtungen unterstützen die sozialen Interessen Bedürftiger.

[0005] Diese und andere wichtige „im Hintergrund" erbrachten Administrations- und Unterstützungsdienste stellen eine Basis bzw. Grundlage dar, welche die Vorteile und Erfordernisse, die für uns ein modernes Leben ausmachen, erst möglich und wirksam machen und eine reibungslose Abwicklung von Geschäften ermöglichen.

[0006] Angenommen, Sie möchten bei Ihrem Bäcker Brot kaufen. Der Bäcker muss nicht alle Schritte erledigen, die zum Brotbacken nötig sind, weil er auf die Unterstützungs- und Administrationsdienste zurückgreifen kann, die die Gemeinschaft erbringt. Zum Beispiel:

- Der Bäcker muss das Korn nicht anbauen und mahlen, um Mehl für das Brot zu erhalten. Vielmehr kann er das Mehl bei einem Anbieter einkaufen, der es mit dem LKW ausliefert.
- Ähnlich muss der Bäcker die zur Beheizung seiner Öfen erforderlichen Brennstoffe nicht selbst anbauen oder gewinnen; der Brennstoff kann in Leitungen oder Tanks durch Personen geliefert werden, die sich auf die Herstellung und Lieferung von Brennstoffen spezialisiert haben.
- Sie können sich auch auf die Sauberkeit in der Bäckerei verlassen, weil dort ein Vermerk über eine Kontrolle durch das örtliche Gesundheitsamt ausgehängt ist.

[0007] Unterstützungs- und Administrationsdienste sind auch erforderlich, um Personen für Ihren Aufwand zu entschädigen. Zum Beispiel:

- Sie und die Bäckerei können sich sicher sein, dass die Regierung hinter der Währung des Geldes steht, das Sie aus Ihrem Portemonnaie oder aus ihrer Geldbörse nehmen, um das Brot zu bezahlen.
- Wenn Sie mit Scheck bezahlen, bucht das Bankensystem den Scheckbetrag über Nacht von ihrem Bankkonto ab und schreibt ihn der Bäckerei gut.
- Sind Sie und die Bäckerei bei verschiedenen Banken, so kann Ihr Scheck durch ein automatisches „Clearinghaus"-System zugestellt werden, mit dessen Hilfe unterschiedliche Banken untereinander Schecks austauschen und Konto-Transaktionen ausführen können – ein effizienter Weg, Geld von Bank zu Bank zu überweisen und Schecks zurückzusenden, deren Konto keine ausreichende Deckung aufweist.

• Akzeptiert die Bäckerei Kreditkarten zur Zahlung, so gestaltet sich die Bezahlung der Backwaren flexibler, und für die Kunden erhöht sich der Komfort beim Kauf sowie ihre Kaufkraft.

[0008] Diese Unterstützungs- und Administrationsdienste erzeugen einen großen Skalen- und Verbundeffekt und machen unsere Wirtschaft effizienter. So kann sich der Bäcker durch diese wichtigen Unterstützungs- und Administrationsdienste auf das konzentrieren, was er am besten kann, nämlich Brot herstellen und backen. Es ist für eine Bäckerei und ihre erfahrenen Bäcker viel wirtschaftlicher, in ihren großen industriellen Öfen viele Brote zu backen, als es für die einzelnen Familien wäre, würden diese ihr Brot in ihrem heimischen Herd selbst backen oder für die Ackerbauern, würden diese das Korn auch noch zu Brot verarbeiten und die zum Backen benötigten Brennstoffe pumpen, und sich in Naturalien auszahlen lassen, etwa Geflügel für Brot. Sie und die Bäckerei können den Kaufvorgang somit mit einer Kreditkarte abschließen, da sowohl Sie als auch die Bäckerei erwarten, dass dieses Zahlungssystem reibungslos arbeitet und erfahrungsgemäß als eine hocheffiziente und komfortable Basis für bargeldlose Transaktionen „automatisch" funktioniert.

Die elektronische Gemeinschaft benötigt Administrations- und Unterstützungsdienste

[0009] Es hat sich mittlerweile eine weltweite elektronische Gemeinschaft herausgebildet. Die Teilnehmer einer elektronischen Gemeinschaft müssen ihre Interaktionen gestalten, steuern und, in einer elektronischen Welt, automatisieren können. Sie sind in hohem Maße von verlässlichen, sicheren und vertrauenswürdigen Unterstützungs- und Administrationsdiensten abhängig.

[0010] Weltweit erfolgen immer mehr Geschäftsabschlüsse elektronisch. Das Internet, ein riesiges elektronisches Netzwerk aus Netzwerken, das Millionen von Rechnern weltweit miteinander verbindet, wird zunehmend als das Medium für geschäftliche Transaktionen verwendet. Größtenteils begünstigt durch benutzerfreundliche Oberflächen (bei denen Verbraucher ihren Einkauf beispielsweise „mit einem Mausklick" auf einen Posten einleiten können, um hiernach ein einfaches Formular auszufüllen, in dem die Kreditkartendaten übermittelt werden), wächst die Bedeutung des Internets als zentrales Instrument für Kunden- und Business-to-Business-Geschäfte rasch. Es entwickelt sich überdies zu einem bedeutenden „Kanal" für den Verkauf und die Verteilung allerlei elektronischer Eigenschaften und Dienste wie Informationen, Software, Spiele und Unterhaltung.

[0011] Gleichzeitig nutzen Großunternehmen private wie öffentliche Datennetzwerke gleichermaßen, um mit ihren Lieferanten und Kunden zu kommunizieren. Bedingt durch scheinbar unaufhaltbar sinkende Kosten für Rechenleistung und Netzkapazität, wird der elektronische Handel an Bedeutung gewinnen, da die Welt zunehmend computerisiert wird. Diese neue elektronische Gemeinschaft generiert durch ihren ausgedehnten elektronischen Handel einen großen Bedarf an elektronischen Administrations-, Unterstützungs- und „Clearing"-Diensten.

[0012] Die elektronische Gemeinschaft bedarf dringend einer Grundlage, die sowohl geschäftliche als auch private elektronische Interaktionen und Beziehungen unterstützt. Elektronischer Handel bedarf ab einer bestimmten Größenordnung eines betriebssicheren, effizienten, skalierbaren und sicheren Netzwerks der Drittanbieterunterstützung und Administrationsdienstleister sowie Mechanismen, die wichtige Transaktionsabläufe erleichtern. Zum Beispiel:

• Personen, die Werte für die elektronische Gemeinschaft bereitstellen, benötigen nahtlose und effiziente Mechanismen der Entschädigung für die von ihnen bereitgestellten Werte.

• Anbieter, die Waren oder Dienstleistungen an die elektronische Gemeinschaft verkaufen, benötigen verlässliche effiziente elektronische Zahlungsmechanismen für sich selbst und andere Teilnehmer der Wertkette.

• Käufer auf dem elektronischen Marktplatz, die oft keine Kenntnisse der komplizierten, hinter einem Überweisungsvorgang steckenden Technologie haben, benötigen dennoch einfach bedienbare, effiziente und flexible Oberflächen zur Betätigung der Zahlungsmechanismen und der zur Erfüllung ihrer finanziellen Verbindlichkeiten nötigen Systeme.

• Rechteinhaber allerlei elektronischer „Inhalte" (zum Beispiel analoger oder digitaler Informationen in Form von Text, Graphiken, Filmen, Animationen, Bildern, Video, digital-linearen Bewegtbildern, Ton- und Tonaufnahmen, Standbildern, Software-Computerprogrammen, Daten) und vieler Arten elektronischer Regelungsabläufe benötigen sichere, flexible und in hohem Maße interoperable Mechanismen zur Verwaltung ihrer Rechte und zur Administration ihrer Geschäftsmodelle, bei Bedarf einschließlich der Einziehung von Zahlungen und der Gewinnung relevanter Daten über die jeweilige Benutzung ihrer Inhalte.

• Alle Parteien sind auf Infrastruktur-Unterstützungsdienste angewiesen, die auch im Falle eines erheblichen Anwachsens der Geschäftsvorgänge zuverlässig, vertrauenswürdig und sicher arbeiten.

[0013] Ein wichtiger Eckpfeiler eines erfolgreichen elektronischen Transaktionsmanagements und Handels besteht daher in der Entwicklung und im Betrieb eines Satzes von Administrations- und Unterstützungsdiensten, die diese Ziele unterstützen und die Entstehung neuer vielfältiger, flexibler, skalierbarer

und effizienter Geschäftsmodelle für den elektronischen Handel im Allgemeinen erleichtern.

Die Patentschrift von Ginter (WO-A-98/09209) beschreibt eine Gesamtlösung

[0014] Die vorgenannte Patentschrift von Ginter et al. beschreibt eine Technologie, die einzigartige leistungsfähige Möglichkeiten bereitstellt, die der Entwicklung eines sicheren, verteilten transaktionsbasierten elektronischen Handels und einer sicheren, verteilten transaktionsbasierten Rechteverwaltung dienlich sind. Diese Technologie kann viele bedeutende neue Geschäftsmodelle und Geschäftsmethoden seitens der Teilnehmer am elektronischen Handel ermöglichen sowie bestehende Geschäftsmodelle und -methoden unterstützen.

[0015] Die Patentschrift von Ginter et al. beschreibt umfassende Gesamtsysteme und eine große Anzahl Verfahren, Techniken, Strukturen und Anordnungen, die einen sicheren, effizienten verteilten elektronischen Handel und eine sichere, effiziente verteilte Rechteadministration im Internet (und in den Intranets) in großen und kleinen Unternehmen, im Wohnraum und im Heimbüro ermöglichen. Diese Techniken, Systeme und Anordnungen haben ein bis dahin unerreichtes Maß an Sicherheit, Zuverlässigkeit, Effizienz und Flexibilität beim elektronischen Handel und bei der elektronischen Rechteverwaltung möglich gemacht.

[0016] Die Patentbeschreibung von Ginter et al. beschreibt überdies ein „Information Utility" – ein Netzwerk aus Unterstützungs- und Administrationsdiensten, Einrichtungen und Anlagen, die die Mechanismen des elektronischen Handels reibungsfreier laufen lassen und elektronische Transaktionen in dieser neuen elektronischen Gemeinschaft unterstützen. Ginter et al. beschreiben beispielsweise eine große Anzahl von Unterstützungs- und Administrationsdienstleistern an der Schnittstelle mit einem von ihnen unterstützten „Virtuellen Verteilungsumgebung". Zu diesen Unterstützungs- und Administrationsdienstleistern gehören u. a.:

- Transaktionsverarbeiter
- Usage Analysts
- Berichtempfänger
- Berichtersteller
- Systemadministratoren
- Berechtigungsagenten
- zertifizierende Behörde
- Content- und Message Repositories (Ablagesysteme für Inhalte und Nachrichten)
- Finanz-Clearinghäuser
- Verbraucher-/Autor-Anmeldesysteme
- Template-Bibliotheken
- Kontrollstrukturbibliotheken
- Auszahlungssysteme
- Systeme für den elektronischen Zahlungsverkehr, Kreditkartensysteme, Systeme für Fakturierung auf Papier und
- Empfangs- Antwort-, Transaktions- und Analyse-Auditsysteme

[0017] XP517588 offenbart ein sicheres Internet-Handels-Protokoll für netzwerkvermittelte digitale Inhalte.

Die vorliegenden Erfindungen bauen auf den Lösungen der Patentschrift von Ginter auf und erweitern diese

[0018] Die vorliegenden Erfindungen bauen auf den in der Patentschrift von Ginter et al. beschriebenen Grundideen auf und erweitern diese Erfindungen, um eine erhöhte Effizienz, Flexibilität und Leistungsfähigkeit bereitzustellen. Sie stellen einen Überbau verteilter elektronischer Administrations- und Unterstützungsdienste bereit (das „Distributed Commerce Utility"). In ihren bevorzugten Ausführungsformen können diese die „Virtuelle Verteilungsumgebung" (und andere in der Patentschrift von Ginter et al. beschriebene Möglichkeiten verwenden und von ihnen profitieren und zu diesen Möglichkeiten übergelagert angeordnet werden und sich auf diese erstrecken.

Kurze Zusammenfassung einiger Merkmale und Vorteile der vorliegenden Erfindungen

[0019] Die vorliegenden Erfindungen stellen eine integrierte, modulare Anordnung aus Administrations- und Unterstützungsdiensten für den elektronischen Handel und für die elektronische Rechteverwaltung und für das elektronische Transaktionsmanagement bereit. Diese Administrations- und Unterstützungsdienste bieten eine sichere Grundlage für Finanzmanagement, Rechteverwaltung, zertifizierende Behörde, Rules Clearing, Usage Clearing, sichere Verzeichnis-Dienste und andere transaktionsbezogene Möglichkeiten, die in einem riesigen elektronischen Netzwerk wie dem Internet und/oder in internen Firmen-Intranets oder sogar in Heimnetzwerken aus elektronischen Geräten betrieben werden.

[0020] Diese Administrations- und Unterstützungsdienste können an die jeweiligen Erfordernisse der Wertketten im elektronischen Handel angepasst werden. Die Teilnehmer des elektronischen Handels können diese Administrations- und Unterstützungsdienste nutzen, um ihre Interessen zu verteidigen, sie können diese Dienste gemäß ihrer Wettbewerbsrealität gestalten und in anderer Form nutzen.

[0021] Die vorliegenden Erfindungen stellen ein "Distributed Commerce Utility" mit einer sicheren, programmierbaren, verteilten Architektur bereit, das Administrations- und Unterstützungsdienste bereitstellt. Das Distributed Commerce Utility kann kommerziell genutzte Administrationsressourcen mit opti-

maler Effizienz nutzen und nach den praktischen Anforderungen dimensionieren, um dem Wachstum im elektronischen Handel Rechnung zu tragen.

[0022] Das Distributed Commerce Utility kann mehrere Commerce Utility Systeme umfassen. Diese Commerce Utility Systeme stellen ein Infrastruktur-Unterstützungsnetz bereit, das von der gesamten elektronischen Gemeinschaft und/oder vielen oder allen ihrer Teilnehmer genutzt oder umgenutzt werden kann.

[0023] Verschiedene Unterstützungsfunktionen können hierarchisch und/oder vernetzt angeordnet werden, um den verschiedenen Geschäftsmodellen und/oder anderen Zielen Rechnung zu tragen. Modulare Unterstützungsfunktionen können in verschiedenen Anordnungen zu verschiedenen Commerce Utility Systemen für verschiedene Design-Implementierungen und Zwecke angeordnet werden. Diese Commerce Utility Systeme können über eine große Anzahl elektronischer Geräte mit unterschiedlichem Verteilungsgrad verteilt werden.

[0024] Das umfassende, von der vorliegenden Erfindung bereitgestellte "Distributed Commerce Utility"

- Ermöglicht einen praktikablen und effizienten elektronischen Handel und eine praktikable und effiziente Rechteverwaltung.
- Stellt Dienste bereit, die elektronische Interaktionen und Konsequenzen sicher administrieren und unterstützen.
- Stellt eine Infrastruktur für den elektronischen Handel und andere Formen elektronischer Interaktion und Beziehungen zwischen Personen bereit.
- Wendet die Nutzeffekte eines modernen verteilten Computer- und Netzwerkbetriebs optimal an.
- Stellt eine elektronische Automatisierung und verteilte Verarbeitung bereit.
- Unterstützt die Infrastruktur des elektronischen Handels und Datenverkehrs, die modular, programmierbar, verteilt und optimal computerisiert ist.
- Stellt eine große Bandbreite an Möglichkeiten bereit, die kombiniert werden können, um Dienste zu unterstützen, die verschiedene Administrations- und Unterstützungsaufgaben erfüllen.
- Maximiert die Vorteile elektronischer Automatisierung und verteilter Verarbeitung für eine optimale Zuweisung und Nutzung von Ressourcen in einem System oder Netzwerk.
- Ist effizient, flexibel, kostengünstig, konfigurierbar, umnutzbar, modifizierbar und verallgemeinerbar.
- Kann den geschäftlichen und privaten Bedürfnissen des Benutzers wirtschaftlich Rechnung tragen.
- Kann Abläufe optimal verteilen, wodurch Handelsmodelle flexibel gestaltet, je nach Bedarf dimensioniert und an die Bedürfnisse der Benutzer angepasst werden können.
- Kann effizient einen kompletten Tätigkeitsbereich und Leistungsumfang bedienen.
- Kann als Mischung verteilter und zentralisierter Abläufe für jedes Geschäftsmodell gestaltet und betrieben werden.
- Stellt eine Mischung lokaler, zentralisierter und vernetzter Möglichkeiten bereit, die individuell gestaltet und umgestaltet werden kann, um so veränderlichen Bedingungen gerecht zu werden.
- Unterstützt Universalressourcen und kann für viele verschiedene Modelle auf jeweils andere Weise verwendet werden; eine bestehende Infrastruktur kann durch verschiedene Wertketten mit verschiedenen Anforderungen auf jeweils andere Weise verwendet werden.
- Kann beliebig viele Handels- und Kommunikationsmodelle unterstützen.
- Wendet lokale, zentralisierte und vernetzte Ressourcen effizient an, um die jeweiligen Anforderungen der betreffenden Wertketten zu erfüllen.
- Die gemeinsame Nutzung von Ressourcen verteilt Kosten und maximiert Effizienz.
- Unterstützt gemischte, verteilte, nach dem Peer-to-Peer-Prinzip arbeitende und zentralisierte vernetzte Möglichkeiten.
- Kann lokal, rechnerfern und/oder zentral betrieben werden.
- Kann synchron, asynchron betrieben werden oder beide Betriebsarten unterstützen.
- Passt sich problemlos und flexibel an die schnelllebigen unzähligen kommerziellen Möglichkeiten, Beziehungen und Grenzen des „Cyberspace" an.

[0025] Insgesamt stellt das Distributed Commerce Utility umfassende integrierte Administrations- und Unterstützungsdienste für einen sicheren elektronischen Handel und andere Formen elektronischer Interaktion bereit.

[0026] Zu den durch die vorliegenden Erfindungen bereitgestellten vorteilhaften Merkmalen und Eigenschaften des Distributed Commerce Utility gehören unter anderem:

- Das Distributed Commerce Utility unterstützt eine programmierbare, verteilte und optimal computerisierte Handels- und Nachrichtenadministration. Es stellt auf einmalige Weise eine Kombination aus Diensten bereit, die verschiedene Administrations- und Unterstützungsaufgaben erfüllen, womit es den für die Erzielung maximaler Vorteile elektronischer Automatisierung, verteilter Verarbeitung und einer System- (beispielsweise Netzwerk-)weiten optimalen Ressourcennutzung erforderlichen administrativen Überbau bereitstellt.
- Das Distributed Commerce Utility ist insbesondere darauf zugeschnitten, die administrative Grundlage für das Internet, Firmen-Intranets und

ähnliche Umgebungen unter Beteiligung von verteilten Erstellern digitaler Informationen, Benutzern und Unterstützungssystemen bereitzustellen.

• Die Architektur des Distributed Commerce Utility stellt eine effiziente, kostengünstige, flexible, konfigurierbare, umnutzbare und verallgemeinerbare Basis für den elektronischen Handel und Administrations- und Unterstützungsdienste im Nachrichtenwesen bereit. Die Bereitstellung dieser Möglichkeiten ist unverzichtbar für die Schaffung einer Basis elektronischer Interaktion zwischen Personen, welche optimale Modelle für die Gestaltung geschäftlicher wie privater elektronischer Beziehungen unterstützt.

• Die Architektur des Distributed Commerce Utility stellt eine Basis für den elektronischen Handel und Unterstützungsdienste im Datenverkehr bereit, die für ein beliebiges spezifisches Modell in einer Mischform aus verteilten und zentralisierten Abläufen gestaltet und betrieben werden kann.

• Die vom Distributed Commerce Utility unterstützten Modelle können in einmaliger Weise gestaltet und umgestaltet werden, um optimale Mischungen lokaler, zentralisierter und vernetzter Administrationsmöglichkeiten des Distributed Commerce Utility progressiv zu reflektieren.

• Die innovativen Möglichkeiten des Distributed Commerce Utility einer elektronischen Administration unterstützen gemischte, verteilte, Peer-to-Peer-basierte und zentralisierte vernetzte Möglichkeiten. Mehrere dieser Möglichkeiten können jeweils in beliebiger Zusammenstellung aus lokalen, externen und zentralen asynchron und/oder synchron vernetzten Kombinationen betrieben werden, die zusammen ein Modell für einen bestimmten Zweck zu bestimmter Zeit ergeben, das im Rahmen des kommerziell Wünschenswerten in höchstem Maße gewerblich anwendbar, wirtschaftlich und marktfähig ist.

• Die Architektur des Distributed Commerce Utility ist universell. Es kann beliebig viele Handels- und Kommunikationsmodelle unterstützen, die entsprechend lokale, zentralisierte und vernetzte Ressourcen teilen (z. B. umnutzen). Somit ermöglicht das Distributed Commerce Utility auf optimale Weise Modelle eines praktikablen und effizienten elektronischen Handels und der Rechteverwaltung, die die Kosten der Ressourcenwartung durch die gemeinsame oder überlappende Benutzung ein- und derselben Ressourcenbasis amortisieren können.

• Ein oder mehrere Handelsmodelle des Distributed Commerce Utility können einige oder alle der Ressourcen eines anderen oder mehrerer anderer Modelle untereinander teilen. Ein oder mehrere Modelle können eine veränderte Mischung und Art ihrer verteilten administrativen Vorgänge hervorbringen, um so den Anforderungen des Cyberspace gerecht zu werden, einem schnelllebigen Raum mit unzähligen kommerziellen Möglichkeiten, Beziehungen und Grenzen.

• Das Distributed Commerce Utility unterstützt die Vorgänge des traditionellen Handels, indem sie dessen Umstellung auf Vorgänge des elektronischen Handels erlaubt. Das Distributed Commerce Utility verbessert des Weiteren diese Vorgänge durch die Verwendung von verteilter Verarbeitung, rechtebezogener "Clearinghaus"-Administration, von Sicherheitsdesigns, objektorientiertem Design, von administrativen Smart-Agents, von Verhandlungs- und elektronischen Entscheidungstechniken und/oder Steuerungstechnik für die elektronische Automatisierung, wie für effiziente, kommerziell praktikable elektronische Handelsmodelle unter Umständen erforderlich.

• Bestimmte Vorgänge des Distributed Commerce Utility (Finanzzahlung, Usage Auditing etc.) können in sicheren Ausführungsumgebungen elektronischer Teilnehmer-/Anwendergeräte ausgeführt werden wie beispielsweise in den in Ginter et al. offenbarten „geschützten Verarbeitungsumgebungen".

• Verteilte Clearinghaus-Vorgänge können über „virtuell vernetzte und/oder hierarchische" Standort-Anordnungen des Commerce Utility Systems ausgeführt werden, die auf einer universellen, interoperablen (beispielsweise nach dem Peer-to-Peer-Prinzip arbeitenden) virtuellen Verteilungsumgebung basieren.

• Für eine bestimmte Anwendung oder ein bestimmtes Modell können verschiedene Anordnungen von Diensten des Distributed Commerce Utility die Vollmacht erhalten, verschiedene Administrations- und/oder Unterstützungsfunktionen bereitzustellen.

• Eine beliebige oder alle der durch das Distributed Commerce Utility unterstützten Aufgaben können durch dasselbe Unternehmen, Konsortium oder andere Unternehmensgruppierungen oder andere Teilnehmer der elektronischen Gemeinschaft wie etwa individuelle Benutzer-Websites ausgeführt und/oder verwendet werden.

• Eine oder mehrere Komponenten des Distributed Commerce Utility können sich aus einem Netzwerk verteilter geschützter Verarbeitungsumgebungen zusammensetzen, die eine oder mehrere Aufgaben in hierarchischer Beziehung und/oder in Peer-to-Peer-Beziehung ausführen.

• Mehrere geschützte Verarbeitungsumgebungen des Distributed Commerce Utility können zur Gesamtfunktion eines Dienstes, einer Basiskomponente und/oder eines Clearinghauses beitragen.

• Verteilte geschützte Verarbeitungsumgebungen, die an der Funktion eines Distributed Commerce Utility beteiligt sind, können in einer bevorzugten Ausführungsform so verteilt sein wie die Anzahl geschützter Verarbeitungsumgebungen von Teilnehmern des VDE (virtual distribution environment, virtuelle Verteilungsumgebung), und/oder

sie können (eine) spezifische hierarchische, vernetzte und/oder zentralisierte Administrations- und Unterstützungs-Beziehung(en) zu diesen geschützten Verarbeitungsumgebungen eines Teilnehmers unterhalten.

• In einem bestimmten Modell kann eine bestimmte oder können mehrere Aufgaben des Distributed Commerce Utility vollständig verteilt werden, bestimmte andere oder eine weitere Aufgabe(n) kann (können) (beispielsweise hierarchisch) zentralisierter und/oder voll zentralisiert sein, und bestimmte andere Aufgaben können partiell verteilt und partiell zentralisiert sein.

• Die durch das Distributed Commerce Utility bereitgestellten elementaren Peer-to-Peer-basierten Steuermöglichkeiten ermöglichen eine beliebige Kombination verteilter Funktionen, die zusammen eine wichtige, praktikable, skalierbare und/oder wesentliche Handelsadministration, Sicherheit und Automatisierungsdienste bereitstellen.

• Kombinationen von Merkmalen, Anordnungen und/oder Möglichkeiten des Distributed Commerce Utility sind in programmierbaren Mischungen verteilter und zentralisierter Anordnungen einsetzbar, wobei verschiedene solcher Merkmale, Anordnungen, und Möglichkeiten in geschützten Verarbeitungsumgebungen von Anwendern und/oder in geschützten Verarbeitungsumgebungen der „mittleren" Basis (lokal, regional, klassenspezifisch etc.) und/oder in geschützten Verarbeitungsumgebungen zentralisierter Dienste betrieben werden.

• Das Distributed Commerce Utility ist zur Unterstützung des Internets und anderer elektronischer Umgebungen mit verteilten Informationserstellern, Benutzern und Dienstleistern besonders zweckmäßig. Indem es Menschen dabei hilft, ihre Aktivitäten in die elektronische Welt zu verlagern, spielt es eine zentrale Rolle bei der Überführung dieser nichtelektronischen Aktivitäten des Menschen in das Internet, die Intranets und andere elektronischen Interaktionsnetzwerke. Diese Netzwerkbenutzer benötigen das Distributed Commerce Utility und Unterstützungsdienste als Basis für die wirtschaftliche Umsetzung ihrer geschäftlichen und privaten Erfordernisse. Diese Basis einer sicheren, verteilten Verarbeitung ist erforderlich, um die Möglichkeiten elektronischer Handelsmodelle optimal dabei zu unterstützen, sich in sinnvoller Weise nach den Anforderungen des Bedarfs zu skalieren und die komplette Palette erforderlicher Aktivitäten und den vollen Leistungsumfang wirtschaftlich zu bewältigen.

• Die von den vorliegenden Erfindungen bereitgestellten Technologien des Distributed Commerce Utility stellen einen Satz sicherer verteilter Unterstützungs- und Administrationsdienste für den elektronischen Handel, Rechteverwaltung, und verteilte Datenverarbeitung und Prozesssteuerung bereit.

• Die Erforderlichkeit von Unterstützungsdiensten des Distributed Commerce Utility einschließlich hochsicherer und ausgereifter technischer und/oder vertraglicher Dienste kann sich aus dem elektronischen Handel und aus Teilnehmern der Wertkette auf nahtlose, komfortable und relativ transparente Art dergestalt ergeben, dass die Benutzer die zugrunde liegende Komplexität ihrer Operationen nicht als Belastung empfinden müssen.

• Das Distributed Commerce Utility kann ein angemessen hohes Niveau im Hinblick auf physische Sicherheit, Computersicherheit, Netzwerksicherheit, Prozess-, Policy-basierte Sicherheit und Automatisierung gewährleisten sowie gleichzeitig eine verbesserte, effiziente, zuverlässige, bedienungsfreundliche, komfortable Funktionalität bereitstellen, die für eine geordnete und effiziente Unterstützung der Bedürfnisse der elektronischen Gemeinschaft erforderlich (oder zumindest äußerst wünschenswert) ist.

• Das Distributed Commerce Utility unterstützt in seinen bevorzugten Ausführungsformen die Schaffung wettbewerbsfähiger Handelsmodelle für den Einsatz in der Umgebung eines „offenen" VDE-basierten digitalen Marktplatzes.

• Das Distributed Commerce Utility kann für die Teilnehmer seiner Wertkette Vorteile und betriebliche Leistungsfähigkeit bereitstellen. Es kann beispielsweise einen vollständigen integrierten Satz wichtiger „Clearingfunktions"-Möglichkeiten bieten, die programmierbar sind und so gestaltet werden können, dass sie Geschäftsbeziehungen mit mehreren Parteien über eine nahtlose, „verteilte" Schnittstelle (beispielsweise eine verteilte Anwendung) optimal unterstützen. Clearing- und/oder Unterstützungsfunktionen und/oder -Sub-Funktionen können nach Bedarf individuell und/oder separat dergestalt zugänglich gemacht werden, dass geschäftlichen Zielen, Vertraulichkeitsinteressen, wirtschaftlichen Zielen oder anderen Zielen Rechnung getragen wird.

• Das Distributed Commerce Utility kann es Anbietern, Kaufleuten, Großhändlern, Umwidmern (Repurposer), Verbrauchern und anderen Teilnehmern der Wertkette leichter machen, Dienste des Distributed Commerce Utility in Anspruch zu nehmen, anzufordern und mit ihnen zu arbeiten. Anschlussmöglichkeiten können einfach, nahtlos und umfassend sein (ein Anschluss kann eine große Bandbreite an Zusatzdiensten bereitstellen).

• Das Distributed Commerce Utility kann ferner Vorteile und Effizienz dadurch verbessern, dass es Verbraucher-Markenimages für durch Teilnehmerunternehmen erbrachte Clearingdienste bereitstellt oder auf andere Weise unterstützt, gleichzeitig aber auf eine gemeinsame Infrastruktur und Abläufe zurückgreift.

• Das Distributed Commerce Utility kann durch

Skalierung und Spezialisierung durch Teilnehmerunternehmen bedeutende Einsparungen erzielen, indem es „virtuelle" Modelle unterstützt, die elektronisch und nahtlos auf Sonderdienste und Möglichkeiten mehrerer Parteien zugreifen.

• Das Distributed Commerce Utility bietet den Verbrauchern komfortable Vorteile wie ein Dienst oder ein Produkt, wobei dieser Dienst oder das Produkt der Nachfrage nach einem „Gewebe" aus verschiedenen Unterstützungsdiensten entspringt – wobei jede dieser Dienste sich aus einem verteilten Gewebe noch weiter spezialisierter Dienste und/oder beteiligter verbundener Dienstleister zusammensetzen kann (das Gesamtgewebe ist für den Teilnehmer der Wertkette sichtbar, die zugrunde liegende Komplexität ist größtenteils oder gänzlich unsichtbar (oder kann es zumindest sein)).

• Dienste und Möglichkeiten des Distributed Commerce Utility können in ihren bevorzugten Ausführungsformen eine oder mehrere beliebige Möglichkeiten einer Virtuellen Verteilungsumgebung wie in Ginter et al. beschrieben verwenden oder auf beliebige sinnvolle Weise mit diesen kombiniert werden wie beispielsweise:

A. VDE-Kette der Verarbeitung und Steuerung,
B. sichere, vertrauenswürdige Kommunikation und Interoperabilität zwischen Knoten,
C. sichere Datenbank,
D. Authentifizierung,
E. verschlüsselt,
F. Fingerprinting,
G. andere VDE-Sicherheitstechniken,
H. Rechte-Betriebssystem (Rights Operating System),
I. Objektdesign und sichere Containertechniken,
J. Container-Kontrollstrukturen,
K. Rechte- und Prozesssteuerungssprache,
L. elektronische Verhandlung,
M. sichere Hardware und
N. Smart-Agent- (Smart-Object-)Techniken (beispielsweise Smart-Agents, eingesetzt als Möglichkeit der Prozesssteuerung, als Gruppen- und/oder andere Administrationsagenten, die die administrative Integration verteilter Knoten unterstützen).

Commerce Utility Systeme können verteilt und kombiniert werden

[0027] Die durch das Distributed Commerce Utility bereitgestellten Unterstützungs- und Administrationsdienst-Funktionen können durch eine elektronische Gemeinschaft, ein elektronisches System oder Netzwerk in verschiedener Weise kombiniert und/oder verteilt werden. Die bevorzugte Ausführungsform verwendet die auf einer geschützten Verarbeitungsumgebung basierte Virtuelle Verteilungsumgebung wie in Ginter et al. beschrieben, um solche Kombinationen und solch eine Verteiltheit zu erleichtern. Da alle derartigen geschützten Verarbeitungsumgebungen einer Virtuellen Verteilungsumgebung zumindest bis zu einem gewissen Grad vertrauenswürdig sind, kann jede geschützte Verarbeitungsumgebung ein Clearinghaus oder Teil eines Clearinghauses sein. Für die Interessen und Bedürfnisse kommerzieller VDE-Knoten-Anwender akzeptable Handelsmodelle können Dienste des Distributed Commerce Utility unterstützen, die bis zu den elektronischen verbraucherseitigen Geräten hin verfügbar sind, indem sie beispielsweise auf andere geschützte VDE-Verarbeitungsumgebungen, sichere Kommunikationstechniken und andere VDE-Möglichkeiten zurückgreifen (wie anderenorts besprochen wird, können VDE-Möglichkeiten direkt in die vorliegenden Erfindungen eingegliedert werden). Solche Geräte können neben stärker zentralisierten Knoten der Wertkette zusammen Kombinationen bilden, die als geschützte Verarbeitungsumgebungen für das virtuelle Clearing fungieren. Das Cyberspace wird somit teilweise von großen „virtuellen" Computern bevölkert, wobei der Zugriff auf Ressourcen auf der Grundlage von „Verfügbarkeit" und Rechten geschieht.

[0028] Das Distributed Commerce Utility ist eine modulare, programmierbare und verallgemeinerbare Umgebung, die solche virtuelle Computer unterstützen kann. Das Distributed Commerce Utility bildet eine einzigartige architekturelle Basis für die Gestaltung von Wertkettenmodellen im elektronischen Handel und virtuellen Computern. Die programmierbare Natur einer bestimmten Implementierung kann wechselnde reale (logische und/oder physische) und/oder Grade der Verteilung für dieselben und/oder ähnliche Dienste unterstützen. Zum Beispiel:

• Zentralisierte Commerce Utility Systeme und Dienste können verwendet werden, um bestimmte Funktionen von Unterstützungsdiensten oder Kombinationen aus Funktionen effizient aus einem zentralisierten Ort bereitzustellen.

• Andere Commerce Utility Systeme könnten in teilweise oder vollständig verteilter Form bereitgestellt werden.

• Manche Funktionen von Unterstützungs- und Administrationsdiensten könnten in und/oder überall in einer bestehenden oder neuen Infrastruktur für den Datenverkehr oder anderen Formen der elektronischen Netzwerkunterstützung verteilt werden.

• Andere Unterstützungsdienste könnten in sicheren Ausführungsumgebungen (beispielsweise geschützten Verarbeitungsumgebungen) mit einem beliebigen elektronischen verbraucherseitigen Gerät oder allen solchen elektronischen verbraucherseitigen Geräten betrieben werden, die Peer-to-Peer-basierten Datenverkehr und Interaktionen verwenden, um beispielsweise das Gewebe eines sicheren Netzes an Unterstützungsdiensten bereitzustellen.

• Andere Unterstützungsdienste könnten sowohl

in der Infrastruktur der Netzwerkunterstützung und als auch in benutzerseitigen elektronischen Geräten betrieben werden.

[0029] Solche verteilten Unterstützungsdienste können stärker zentralisierte Installationen von Unterstützungsdiensten ergänzen (und/oder überflüssig machen). Unterschiedliche Kombinationen derselben und/oder abweichende, nicht verteilte und unterschiedlich verteilte Dienste können bereitgestellt werden, um verschiedene Aktivitäten zu unterstützen. Ferner kann die Art und Verteilung von Diensten für ein Gesamtmodell zwischen den einzelnen Implementierungen differieren. Solche differierenden Modellimplementierungen können bei Bedarf sowohl dieselben Commerce Utility Systeme als auch Dienste und/oder jede bestimmte und/oder jede Kombination aus Administrations- und/oder Unterstützungsfunktionen des Distributed Commerce Utility untereinander teilen.

[0030] Ferner kann eine bestimmte Infrastruktur von Commerce Utility Systemen und Diensten durch unterschiedliche Wertketten (z. B. ein Geschäftsmodell oder ein Satz Beziehungen) auf unterschiedliche Art und Weise verwendet werden. So können etwa bestimmte Wertketten es vorziehen, bestimmte Funktionen von Unterstützungsdiensten aus Gründen der Effizienz, Sicherheit, Steuerung oder aus anderen Gründen stärker zentralisiert zu gestalten, andere können hingegen stärker und/oder anders verteilte Modelle bevorzugen.

[0031] Sofern beispielsweise Zahlungsmethoden und Rechteinhaber und/oder andere Teilnehmer der Wertkette übereinstimmen, können beliebige oder mehrere der Unterstützungsdienste einer sicheren Infrastruktur eines Distributed Commerce Utility einen Teil ihrer Funktionen oder alle ihre Funktionen und Rechte über eine beliebige Auswahl oder einen beliebigen Satz elektronischer Geräte von Endanwendern und/oder anderen Wertketten verteilen und/oder delegieren. Die Verteilung und Übertragung dieser Dienste und Funktionen bietet verschiedene Vorteile wie beispielsweise die Ermöglichung einer flexiblen und effizienten Schaffung temporärer Ad-hoc-Netze des sicheren elektronischen Handels, in denen ein beliebiges, einige oder alle Gerät(e) in der Auswahl oder in dem Satz mindestens als partieller (oder gar als vollständiger) Peer anderer Geräte in demselben Handelsnetzgewebe teilnehmen kann.

[0032] Die vorliegende Erfindung stellt unter anderem die folgenden zusätzlichen Merkmale der Verteilung von Administrations- und Unterstützungsfunktionen bereit:

- Eine beliebige Mischung aus beliebigen Administrations- und/oder Unterstützungsfunktionen kann in eine andere Mischung aus Administrations- und/oder Unterstützungsfunktionen eingegliedert werden.
- Ein beliebiger Satz oder eine Teilmenge an Funktionen eines Commerce Utility Systems kann in einer integrierten Ausführung mit einer beliebigen anderen Mischung von Funktionen eines Commerce Utility Systems kombiniert werden. Solche Mischungen können zu einem beliebigen gewünschten Grad verteilt werden, und ein beliebiger Abschnitt oder mehrere Abschnitte der Mischung können stärker oder schwächer als ein beliebiger anderer Abschnitt oder mehrere andere Abschnitte verteilt werden. Hierdurch stehen einer Wertkette optimal gewünschte und/oder praktikable Ausführungen zur Verfügung. Es kann eine beliebige Mischung einschließlich beliebiger Verteilungsgrade des Rechte-Clearings, Finanzclearings, Usage Aggregation, Usage Reporting und/oder anderer Funktionen des Clearings und/oder Distributed Commerce Utility bereitgestellt werden. Solche Funktionen eines Distributed Commerce Utility und/oder solche Administrations- und/oder Unterstützungsdienste können mit beliebigen anderen gewünschten Funktionen eines Distributed Commerce Utility und/oder mit beliebigen anderen gewünschten Administrations- und/oder Unterstützungsdiensten kombiniert werden.
- Ein beliebiger oder mehrere solche Administrations- und/oder Unterstützungsdienste und/oder -funktionen können als Commerce Utility System betrieben werden und ein Netz aus Commerce Utility System-Knoten unterstützen, von denen jeder mindestens einen Teil solcher Administrationsdienstaktivitäten eines Commerce Utility unterstützt. Jedes Commerce Utility System kann in der Lage sein, Rechte und/oder Dienste für andere Commerce Utility Systeme und/oder Knoten bereitzustellen und/oder mit diesen anderweitig sicher zu interoperieren.
- Jedes Commerce Utility System (oder jede Kombination aus Commerce Utility Systemen) kann in der Lage sein, als ein „virtuelles Clearinghaus" aus mehreren Commerce Utility Systemen teilzunehmen. In der bevorzugten Ausführungsform können diese „virtuelle Clearinghäuser", wenn in Übereinstimmung mit VDE-Regeln und Steuermechanismen, in der durch solche Regeln und Steuermechanismen vorgeschriebenen Weise mit anderen Commerce Utility Systemen und/oder anderen virtuellen, in demselben Netz teilnehmenden Clearinghäusern interoperieren. Solche „virtuellen Clearinghäuser" können Berechtigungen von einer sicheren Kette der Verarbeitung und Steuerung in Form elektronischer Regelsätze erhalten, und können an der aus dieser Kette der Verarbeitung und Steuerung und anderen VDE-Möglichkeiten resultierenden Prozessautomatisierung im elektronischen Handel teilnehmen.

[0033] Diese Möglichkeit, beliebige Funktionen von Unterstützungsdiensten zu einem beliebigen gewünschten Grad in einem System oder Netzwerk zu verteilen und bei Bedarf hiernach anzupassen (zu modifizieren), stellt einen großen Zuwachs an Leistung, Flexibilität und Effizienz bereit. Beispielsweise werden Verteilungsaspekte von Unterstützungsdiensten wie Clearingfunktionen helfen, solche „Engpässe" zu vermeiden, die beim Einsatz einer zentralisierten Clearingeinrichtung dadurch entstehen würden, dass die für eine Bewältigung der zu verarbeitenden Daten erforderlichen Kapazitäten fehlen. Die Nutzung der Vorteile verteilter Verarbeitungsleistung einer großen Anzahl Teilnehmergeräte in der Wertkette bietet überdies große Vorzüge mit Hinblick auf eine erhöhte Effektivität und Reaktionszeit des Systems, wesentlich geringere allgemeine Betriebskosten, eine größere Fehlertoleranz, vielseitige Möglichkeiten der Anwendungsimplementierung und dank der Anpassungsfähigkeit der vorliegenden Erfindungen an die Bedürfnisse und Anforderungen der jeweiligen Teilnehmer der Wertkette allgemein eine wesentlich größere Attraktivität für die Wertkette.

Einige Beispiele für die durch das Distributed Commerce Utility bereitgestellten Administrations- und/oder Unterstützungsdienste

[0034] Das Distributed Commerce Utility kann in einer Anzahl verschiedener spezieller und/oder universeller „Commerce Utility Systeme" organisiert sein. Die Commerce Utility Systeme können zentralisiert, verteilt oder partiell verteilt und partiell zentralisiert werden, um die für die Verwaltungsebene des Handels in der Praxis erforderlichen Administrationsdienste, Sicherheitsdienste, und andere Dienste bereitzustellen. Bestimmte Commerce Utility Systeme enthalten auf einem Distributed Commerce Utility basierende Implementierungen gängiger Funktionen von Administrationsdiensten wie etwa Finanz-Clearinghaus und zertifizierende Behörden. Andere Commerce Utility Systeme beinhalten neue Dienstformen und neue Kombinationen und Anordnungen für bekannte Dienstleistungsaktivitäten. Ein Commerce Utility System ist eine beliebige Instantiierung des Distributed Commerce Utility, die ein spezifisches elektronisches Handelsmodell unterstützt, und ein Commerce Utility System kann selbst aus mehreren Commerce Utility Systemen zusammengesetzt sein. Commerce Utility Systeme können jeden oder alle der nachstehenden Punkte in jeder Kombination von Möglichkeiten und Verteilungsanordnungen umfassen, zum Beispiel:

- Finanz-Clearinghäuser,
- Usage-Clearinghäuser,
- Rechte- und Berechtigungs-Clearinghäuser,
- zertifizierende Behörden
- sichere Verzeichnis-Dienste,
- sichere Transaktionsberechtigungen,
- multifunktionale, universelle und/oder kombinierte Commerce Utility Systeme einschließlich einer beliebigen Kombination der Möglichkeiten der unmittelbar vorstehend genannten Systeme und
- andere Commerce Utility Systeme.

[0035] Diese Commerce Utility Systeme sind hinsichtlich ihres Nutzens und ihrer Anwendbarkeit weit reichend. Sie können beispielsweise eine administrative Unterstützung für jeden oder alle der nachstehenden Punkte bereitstellen:

- vertrauenswürdiges elektronisches Ereignismanagement,
- vernetzte, automatische, verteilte, sichere Prozessadministration und -steuerung,
- Verarbeitungskette und -steuerung einer Virtuellen Verteilungsumgebung und
- Rechteadministration und Usage- (beispielsweise Ereignis-) Management (beispielsweise Auditing, Steuerung, Rechteerfüllung etc.), netzwerkübergreifend und/oder innerhalb elektronischer Netzwerke einschließlich „nicht angeschlossener", virtuell angeschlossener oder periodisch angeschlossener Netzwerke.

[0036] Die Commerce Utility Systeme können elektronische Prozessketten und elektronische Ereignis-Konsequenzen in beispielsweise den folgenden Bereichen regeln:

- elektronische Werbung,
- Markt- und Benutzungsanalyse,
- elektronische Währung,
- Transaktionsclearing und Datenverkehr im Finanzwesen,
- Fertigung und andere Modelle verteilter Prozesssteuerung
- Finanzclearing,
- Ermöglichung von Zahlungserfüllung oder Bereitstellung anderer Formen der Entschädigung (einschließlich Bearbeitungsgebühren, Produktgebühren oder beliebige andere Gebühren und/oder Vergütungsleistungen) zumindest teilweise auf der Grundlage von Inhaltsverwaltung (Content Management), Prozesssteuerungs-Management (Ereignismanagement) und/oder Rechteverwaltung,
- Durchführung von Audits, Fakturierung, Zahlungserfüllung (oder Bereitstellung anderer Formen der Entschädigung) und/oder andere Clearingaktivitäten,
- Kompilierung, Aggregation, Verwendung und/oder Bereitstellung von Informationen in Bezug auf die Verwendung eines oder mehrerer sicherer Container und/oder Inhalte und/oder Abläufe (Ereignisse) einschließlich Inhalte sicherer Container und/oder eines beliebigen anderen Inhalts,
- Bereitstellung von Informationen auf der Grundlage von Usage Auditing, Benutzerprofil-Erstellung und/oder Marktuntersuchung in Bezug auf die Benutzung eines oder mehrerer sicherer Con-

tainer und/oder Inhalte und/oder Abläufe (Ereignisse),
• Benutzung von Informationen, die beim Benutzerkontakt mit Inhalten (einschließlich Werbung) gewonnen wurden und/oder die Verwendung von Vorgängen (Ereignissen),
• Bereitstellung von Objekt-Registry-Diensten; und/oder Informationen zu Rechten, Berechtigungen, Preisen und/oder anderen Regeln und Steuermechanismen; für registrierte und/oder registrierende Objekte;
• elektronische Zertifizierung von Informationen, die im Zusammenhang mit Regeln und Steuermechanismen verwendet und/oder für diese benötigt werden, wie Authentifizierung der Identität, Klassenzugehörigkeit und/oder anderer Attribute im Identitätskontext einschließlich beispielsweise Zertifizierung der Klassenidentität für Automatisierungsabläufe, wie etwa rechtebezogene Erfüllung von Finanztransaktionen auf der Grundlage geltender Rechtsprechung (Steuer(n)), Beschäftigung und/oder anderer Gruppenzugehörigkeit einschließlich beispielsweise erworbener Klassenrechte (beispielsweise Clubmitgliedschaft von Diskontkäufern);
• Archivierung und/oder Authentifizierung von Transaktionen und/oder Transaktionsdaten durch Dritte für ein sicheres Backup und Nichtrückweisbarkeit (non-repudiation),
• Bereitstellung programmierter gemischter Anordnungen von Diensten der Prozesssteuerung und Automatisierung eines Commerce Utility Systems, wobei unterschiedliche Commerce Utility Systeme die Anforderungen unterschiedlicher Wertketten und/oder Geschäftsmodelle unterstützen, und wobei solche Commerce Utility Systeme ferner verteilte, skalierbare, effiziente vernetzte und/oder hierarchische feste und/oder virtuelle Clearinghausmodelle unterstützen, die einen sicheren Datenverkehr zwischen den geschützten Verarbeitungsumgebungen der verteilten Clearinghäuser eines Commerce Utility Systems verwenden, um Clearinghausbezogene Regeln und Steuermechanismen und abgeleitete, zusammengefasste und/oder detaillierte Transaktionsdaten zu übermitteln,
• EDI (Electronic Data Interchange, elektronischer Datenaustausch), elektronische Handelsmodelle und verteilte Anordnungen der Datenverarbeitung, in denen Teilnehmer eine vertrauenswürdige Basis benötigen, die eine effiziente, verteilte Administration, Automatisierung, und Steuerung von Transaktions-Wertketten ermöglicht, und
• andere Unterstützungs- und/oder Administrationsdienste und/oder -funktionen.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0037] Diese und weitere durch die vorliegenden Erfindungen bereitgestellten Merkmale und Vorteile werden besser und vollständiger verständlich, wenn die folgende detaillierte Beschreibung der derzeit bevorzugten Ausführungsbeispiele zusammen mit den Zeichnungen hinzugezogen wird; hierbei:

[0038] zeigt Fig. 1 ein Beispiel für ein Distributed Commerce Utility, das ein exemplarisches elektronisches Verbrauchergerät unterstützt;

[0039] zeigt Fig. 1A (eine) geschützte Verarbeitungsumgebunge(n) („PPE", protected processing environment) innerhalb des elektronischen Verbrauchergeräts (der elektronischen Verbrauchergeräte);

[0040] zeigt Fig. 1B, dass das Distributed Commerce Utility mehrere exemplarische Commerce Utility Systeme enthalten kann;

[0041] zeigen Fig. 2A-Fig. 2E am Beispiel, wie Funktionen von Administrations- und Unterstützungsdiensten verteilt werden können;

[0042] zeigen Fig. 3A-Fig. 3C Beispiele für Distributed Commerce Utility Systeme;

[0043] zeigt Fig. 4 ein exemplarisches Netz von Commerce Utility Systemen;

[0044] zeigt Fig. 4A ein uneingeschränktes Netz von Verbrauchergeräten und Commerce Utility Systemen;

[0045] zeigt Fig. 5, wie Rechteinhaber zwischen mehreren, an eine „Datenautobahn" angeschlossenen, Commerce Utility Systeme wählen können;

[0046] zeigt Fig. 6 am Beispiel, wie verschiedene Commerce Utility Systeme zusammenarbeiten können;

[0047] zeigt Fig. 7 am Beispiel, wie multiple Funktionen von Administrations- und Unterstützungsdiensten in Commerce Utility Systeme kombiniert und integriert werden können;

[0048] zeigt Fig. 7A ein Beispiel für ein Netz aus Commerce Utility Systemen mit kombinierter Funktion;

[0049] zeigen Fig. 8A-Fig. 8B Beispiele für Hierarchien eines Commerce Utility Systems;

[0050] zeigt Fig. 9 ein Beispiel für eine Hierarchie multifunktionaler Commerce Utility Systeme

[0051] zeigt Fig. 10 ein Beispiel für ein Finanz-Clearinghaus;

[0052] zeigt Fig. 11 ein Beispiel für ein Usage-Clearinghaus;

[0053] zeigt Fig. 12 ein Beispiel für ein Rechte- und Berechtigungs-Clearinghaus;

[0054] zeigt Fig. 13 ein Beispiel für eine zertifizierende Behörde;

[0055] zeigt Fig. 14 ein Beispiel für einen sicheren Verzeichnis-Dienst;

[0056] zeigt Fig. 15 ein Beispiel für eine Transaktionsbehörde;

[0057] zeigen Fig. 16A-Fig. 16F, dass Commerce Utility Systeme andere Utility-Systeme im Handel unterstützen können;

[0058] zeigen Fig. 17A bis Fig. 17D-3 ein Beispiel für die Architektur eines Commerce Utility Systems;

[0059] zeigen Fig. 17E-1 bis Fig. 17E-4 Beispiele für Interaktionsmodelle eines Commerce Utility Systems;

[0060] zeigt Fig. 17F eine exemplarische Anordnung für die Verteilung von Teilen der Vorgänge eines Administrations- und Unterstützungsdienstes;

[0061] zeigt Fig. 18 ein exemplarisches Commerce Utility System eines Finanzclearinghauses;

[0062] zeigt Fig. 19 eine exemplarische Anordnung für ein Finanz-Clearinghaus;

[0063] zeigt Fig. 20 einen exemplarischen Ablauf beim Finanzclearing;

[0064] zeigen Fig. 20A-Fig. 20F ein zusätzliches Beispiel für Aktivitäten und Abläufe des Finanzclearing;

[0065] zeigt Fig. 21 ein vereinfachtes Beispiel für die Disaggregation einer Wertkette (Bezahlung);

[0066] zeigt Fig. 22 am Beispiel, wie die Disaggregation gemäß Fig. 21 in der Umgebung eines Finanz-Clearinghauses implementiert werden kann;

[0067] zeigt Fig. 22A eine exemplarische Anordnung für die Implementierung einer Bezahlungs-Disaggregation in der geschützten Verarbeitungsumgebung des Benutzers;

[0068] zeigt Fig. 23 ein Beispiel für die Disaggregation einer komplexeren Wertkette (Bezahlung);

[0069] zeigt Fig. 24 am Beispiel, wie Disaggregation in der Umgebung eines Finanz-Clearinghäuser implementiert werden kann;

[0070] zeigt Fig. 25 ein Beispiel für die Disaggregation einer Wertkette mit Angaben zur Kompensation für das Distributed Commerce Utility;

[0071] zeigt Fig. 26 exemplarisch die Disaggregation einer Wertkette (Bezahlung) an beliebig viele Zahlungsempfänger;

[0072] zeigt Fig. 27 an einem weiteren Beispiel, wie die Disaggregation einer Wertkette (Bezahlung) und der Redistribution durch ein Finanz-Clearinghaus erreicht werden kann;

[0073] zeigt Fig. 28 ein exemplarisches Szenario für Superdistributionszahlung und Redistribution unter Verwendung eines Finanz-Clearinghauses für Finanzclearing;

[0074] zeigt Fig. 29 eine exemplarische Aggregation einer Wertkette (Bezahlung) in einer geschützten Verarbeitungsumgebung oder anderen Umgebung des Verbrauchers;

[0075] zeigt Fig. 30 eine exemplarische Aggregation einer Wertkette (Bezahlung) über Mehrfachtransaktionen;

[0076] zeigt Fig. 31 eine exemplarische Aggregation einer Wertkette (Bezahlung) über Mehrfachtransaktionen und mehrere Verbraucher;

[0077] zeigt Fig. 32 ein Beispiel für die Architektur eines Commerce Utility Systems, das eine Zahlungsaggregation bereitstellt;

[0078] zeigt Fig. 33 exemplarisch ein aus Usage-Clearinghäusern bestehendes Commerce Utility System;

[0079] zeigt Fig. 34 ein Beispiel für die Architektur eines Usage-Clearinghauses;

[0080] zeigt Fig. 35 einen exemplarischen Ablauf beim Usage-Clearing;

[0081] zeigt Fig. 36 einen weiteren exemplarischen Ablauf beim Usage-Clearing unter Verwendung mehrerer Usage-Clearinghäuser;

[0082] zeigt Fig. 37 einen exemplarischen Ablauf beim Usage-Clearing unter Verwendung von Usage- und Finanz-Clearinghäusern;

[0083] zeigt Fig. 38 einen exemplarischen Ablauf der Medienplatzierung im Usage-Clearinghaus;

[0084] zeigt Fig. 39 einen exemplarischen Ablauf beim Usage-Clearing, der auf der Grundlage von verschiedenen Ebenen der Offenlegung von Benutzungsinformationen durch den Verbraucher Rabatte bereitstellt;

[0085] zeigt Fig. 40 ein Beispiel für ein Commerce Utility System vom Typ eines Rechte- und Berechtigungs-Clearinghauses;

[0086] zeigt Fig. 41 ein Beispiel für die Architektur eines Rechte- und Berechtigungs-Clearinghauses;

[0087] zeigt Fig. 42 einen exemplarischen Clearingablauf für Rechte und Berechtigungen;

[0088] zeigt Fig. 42A ein Beispiel für den Ablauf der Registrierung eines Regelsatzes für Updates;

[0089] zeigt Fig. 43 einen weiteren exemplarischen Clearingablauf für Rechte und Berechtigungen;

[0090] zeigen Fig. 44A-Fig. 44E ein weiteres Beispiel für Rechte- und Berechtigungs-Clearing;

[0091] zeigen Fig. 45A und Fig. 45B exemplarische Rechtetemplate(s);

[0092] Fig. 45C zeigt ein Beispiel für einen mit dem (den) exemplarischen Rechtetemplate(s) korrespondierenden Regelsatz;

[0093] zeigt Fig. 46 ein weiteres Beispiel für einen Rechte- und Berechtigungs-Clearingablauf;

[0094] zeigt Fig. 47 ein exemplarisches Commerce Utility System einer zertifizierenden Behörde;

[0095] zeigt Fig. 48 eine exemplarische Architektur einer zertifizierenden Behörde; Fig. 49 zeigt ein Beispiel für einen Zertifizierungsablauf;

[0096] zeigt Fig. 50 ein Beispiel für einen verteilten Zertifizierungsablauf;

[0097] zeigt Fig. 50A ein Beispiel für einen Regelsatz, der Leistung und/oder andere Konsequenzen vom Vorhandensein digitaler Zertifikate abhängig macht;

[0098] zeigen Fig. 51A-Fig. 51D ein Beispiel für Datenstrukturen digitaler Zertifikate;

[0099] zeigt Fig. 51E eine exemplarische Technik für die Erzeugung digitaler Zertifikate auf der Grundlage anderer digitaler Zertifikate und (einer) vertrauenswürdiger(n) Datenbank(en);

[0100] zeigen Fig. 51F-Fig. 51H eine exemplarische Technik für die Definition einer virtuellen Einheit;

[0101] zeigt Fig. 52 ein Beispiel für ein Commerce Utility System für sichere Verzeichnis-Dienste;

[0102] zeigt Fig. 53 eine exemplarische Architektur für sichere Verzeichnis-Dienste;

[0103] zeigt Fig. 54 einen exemplarischen Ablauf für sichere Verzeichnis-Dienste;

[0104] zeigt Fig. 55 ein Beispiel für ein Commerce Utility System einer Transaktionsbehörde;

[0105] zeigt Fig. 56 ein Beispiel für eine Architektur einer Transaktionsbehörde;

[0106] zeigt Fig. 57 einen exemplarischen Ablauf in einer Transaktionsbehörde;

[0107] zeigt Fig. 58A am Beispiel, wie die Transaktionsbehörde ein Regel-Superset erstellt;

[0108] zeigt Fig. 58B exemplarisch durch die Transaktionsbehörde ausgeführte Schritte;

[0109] zeigen Fig. 58C und Fig. 58D ein Beispiel für ein Commerce Utility System mit einem sicheren Prüfpunkt;

[0110] zeigen Fig. 59 und Fig. 60 am Beispiel, wie das Distributed Commerce Utility verschiedene elektronische Wertketten unterstützen kann,

[0111] zeigt Fig. 61 ein Beispiel für Einkauf, Lizenzierung und/oder Vermietung;

[0112] zeigt Fig. 62 ein Beispiel für den Einkauf und die Bezahlung eines materiellen Artikels;

[0113] zeigt Fig. 63 ein Beispiel dafür, wie ein Kunde sicher für Leistungen bezahlt;

[0114] zeigt Fig. 64 exemplarisch die Disaggregation einer Wertkette für den Einkauf materieller Güter;

[0115] zeigt Fig. 65 ein Beispiel für die Kooperation zwischen Commerce Utility Systemen innerhalb und außerhalb eines Unternehmens;

[0116] zeigt Fig. 66 ein Beispiel für eine Transaktionsbehörde innerhalb eines Unternehmens und zwischen Unternehmen;

[0117] zeigt Fig. 67 ein Beispiel für den internationalen Handel.

DETAILLIERTE BESCHREIBUNG DER AUSFÜHRUNGSBEISPIELE

Distributed Commerce Utility

[0118] Fig. 1 zeigt ein Beispiel für ein Verbrauchergerät **100**, das an ein Distributed Commerce Utility **75** elektronisch angeschlossen ist. In diesem Beispiel verbindet ein elektronisches Netzwerk **150** das Gerät **100** mit einem Distributed Commerce Utility **75**. Das Distributed Commerce Utility **75** unterstützt die im

Verbrauchergerät **100** stattfindenden Aktivitäten.

[0119] Das Distributed Commerce Utility **75** stellt eine Basis von Administrations- und Unterstützungsdiensten für den elektronischen Handel und Datenverkehr bereit. Diese Basis ist effizient, kostengünstig, flexibel, konfigurierbar, umnutzbar, programmierbar und verallgemeinerbar. Sie unterstützt alle möglichen elektronischen Beziehungen, Interaktionen und Formen des Datenverkehrs sowohl für den privaten als auch für den geschäftlichen Gebrauch.

Das Distributed Commerce Utility kann beliebige elektronische Geräte unterstützen

[0120] Gerät **100** kann ein beliebiges elektrisches oder elektronisches Gerät wie beispielsweise ein Computer, ein Unterhaltungssystem, ein Fernseher oder ein Videoplayer sein, um nur einige Beispiele zu nennen. Im konkreten Beispiel von Fig. 1 ist das Verbrauchergerät **100** ein Heim-Farbfernseher **102**, ein Videoplayer/-recorder **104**, und eine Set-Top-Box **106**. Gerät **100** kann beispielsweise durch die Handfernsteuerung **108** gesteuert werden. Die Set-Top-Box **106** könnte beispielsweise Fernsehprogramme von Fernseh-Sendeanstalten **110** und/oder Satelliten **112** über ein Kabel-TV-Netzwerk **114** empfangen. Der Player/Recorder **104** könnte verschiedene Arten Sendungsmaterial von Bändern, optischen Disks oder anderen Medien wiedergeben und kann überdies über die Fähigkeit verfügen, über die Set-Top-Box **106** empfangenes Sendungsmaterial aufzuzeichnen.

Das Gerät **100** kann über eine "geschützte Verarbeitunpsumgebung" verfügen

[0121] Gerät **100** ist vorzugsweise ein sicheres elektronisches Gerät des beispielsweise in den Fig. 7 und 8 der Patentschrift von Ginter et al. gezeigten Typs. Es ist vorzugsweise Teil der „Virtuellen Verteilungsumgebung" wie in der Patentschrift von Ginter et al. beschrieben. Fig. 1A zeigt, dass Fernseher **102**, Set-Top-Box **106**, Medienspieler/-recorder **104** und Fernbedienung **108** jeweils eine „geschützte Verarbeitungsumgebung"" („PPE") **154** haben können. Das Distributed Commerce Utility **75** kann mit den jeweils innerhalb dieser geschützten Verarbeitungsumgebungen **154** stattfindenden Vorgängen interagieren und diese unterstützen.

[0122] Geschützte Verarbeitungsumgebungen **154** können auf einem oder mehreren Computerchips wie einer Hardware- und/oder Softwarebasierten „sicheren Verarbeitungseinheit" gemäß Fig. 9 der Patentschrift von Ginter et al. basieren. Die geschützte Verarbeitungsumgebung **154** stellt eine hochsichere vertrauenswürdige Umgebung bereit, in der elektronische Abläufe und Transaktionen sicher und ohne erhebliche Manipulationsgefahren von außen oder andere Beeinträchtigungen ausgeführt werden können. Die Offenbarung des Patents von Ginter et al. beschreibt Techniken, Systeme und Verfahren für den Entwurf, die Konstruktion und die Wartung der geschützten Verarbeitungsumgebung **154** dergestalt, dass der Rechteinhaber und andere Teilnehmer der Wertkette (einschließlich Verbraucher **95**) auf ihre Sicherheit und Integrität vertrauen können. In der bevorzugten Ausführungsform ist diese Vertrauenswürdigkeit bei der Interaktion zwischen dem Distributed Commerce Utility **75** und dem elektronischen Gerät **100** wichtig.

Das Distributed Commerce Utility kann sich aus vielen "Commerce Utility Systemen" zusammensetzen

[0123] Fig. 1B zeigt, dass das Distributed Commerce Utility **75** aus mehreren Commerce Utility Systemen **90** zusammensetzt sein kann. Commerce Utility Systeme können in verschiedener Form auftreten, beispielsweise in Form:

- eines Finanz-Clearinghauses **200**;
- eines Usage-Clearinghauses **300**;
- eines Rechte- und Berechtigungs-Clearinghauses **400**;
- einer zertifizierenden Behörde **500**;
- sicherer Verzeichnis-Dienste **600**;
- einer Transaktionsbehörde **700**;
- eines VDE-Administrators **800**; und
- anderer Commerce Utility Systeme **90**.

[0124] Commerce Utility Systeme **90** können Funktionen oder Vorgänge innerhalb einer geschützten/innerhalb geschützter Verarbeitungsumgebung(en) **154** unterstützen und administrieren. Beispielsweise:

- Die geschützte Verarbeitungsumgebung **154** von Gerät **100** kann einen automatischen elektronischen Zahlungsmechanismus **118** bereitstellen, der je nach in Anspruch genommenen Sendungen von der Bank oder einem anderen Geldkonto des Verbrauchers Geldbeträge einzieht. Das Distributed Commerce Utility **75** kann ein spezielles Commerce Utility System **90a** umfassen, genannt „Finanz-Clearinghaus" **200**, das finanzielle Aspekte des Betriebs der geschützten Verarbeitungsumgebung **154** unterstützt und damit sicherstellt, dass Rechteinhaber und andere die korrekten Beträge ausgezahlt bekommen und die Verbraucher **95** nicht zu viel zahlen.
- Die Sendeanstalt eines Fernsehprogramms **102a** kann fordern, dass die geschützte Verarbeitungsumgebung **154** von Gerät **100** mit einem elektronischen Benutzungs-Zählmechanismus **116** misst, wie viel sich die Verbraucher **95** vom Videoprogramm **102a** ansehen, und welche Videoprogramme sie sehen. Das Distributed Commerce Utility **75** kann ein spezielles Commerce Utility System **90b** umfassen, genannt „Usage-Clearinghaus" **300**, das durch einen Benutzungszähler **116** innerhalb der geschützten Verarbeitungsum-

gebung **154** gemessene Benutzungsdaten empfängt, analysiert, und Berichte bereitstellt.

• Der Rechteinhaber am Videoprogramm **102a** kann darauf bestehen, dass die geschützte Verarbeitungsumgebung **154** einen Kopierschutzmechanismus **120** bereitstellt, der Videoprogramm **102a** sicher gegen Kopieren schützt. Das Distributed Commerce Utility **75** kann ein spezielles Commerce Utility System **90c** umfassen, genannt „Rechte- und Berechtigungs-Clearinghaus" **400**, das die geschützte Verarbeitungsumgebung **154** mit solchen Berechtigungen ausstattet, die dafür erforderlich sind, dass der Verbraucher **95** bestimmte Sendungen (beispielsweise auf Pay-per-View-Grundlage) sehen kann, und das bei der Durchsetzung von Verboten Hilfestellung leistet, beispielsweise mithilfe eines Kopierschutzmechanismus **120**.

• Rechteinhaber am Videoprogramm **102a** können ferner verlangen, dass die geschützte Verarbeitungsumgebung **154** von Gerät **100** ein „digitales Zertifikat" **122** besitzt, das Identität und Alter des Verbrauchers oder ähnliche Verbraucherdaten zertifiziert, bevor Verbraucher **95** das Videoprogramm **102a** sehen können. Das Distributed Commerce Utility **75** kann ein spezielles Commerce Utility System **90d** umfassen, genannt "zertifizierende Behörde" **500**, das „digitale Zertifikate" **504** für die geschützte Verarbeitungsumgebung **154** erstellt und bereitstellt, wodurch die Verbraucher mit den durch die Rechteinhaber bereitgestellten Berechtigungen effizient interagieren können.

[0125] Weitere in Fig. 1B gezeigte Commerce Utility Systeme **90** umfassen:

• „Sichere Verzeichnis-Dienste" **600**, die die geschützte Verarbeitungsumgebung **154** beim elektronischen Datenaustausch mit anderen Computern und Geräten in Netzwerk **150** unterstützen können;

• Eine „Transaktionsbehörde" **700**, die für Vorgänge der Prozesssteuerung und -automatisierung zur Verfügung stehen kann wie beispielsweise sicheres Auditieren und sichere Überwachung komplizierter elektronischer Transaktionen unter Beteiligung einer geschützten Verarbeitungsumgebung **154**; und

• Einen „Administrator" **800** einer virtuellen Verteilungsumgebung („VDE"), der in der bevorzugten Ausführungsform einen reibungslosen und sicheren Betrieb der geschützten Verarbeitungsumgebung **154** gewährleisten kann.

[0126] Es können weitere, in Fig. 1B nicht dargestellte Commerce Utility Systeme **90** verwendet werden, um zusätzliche Funktionen und Vorgänge zu administrieren und/oder unterstützen. Die verschiedenen Commerce Utility Systeme **90** können zusammenarbeiten und die Gesamtaufgaben untereinander aufteilen, um die Verbraucher **95** effizient und effektiv zu unterstützen.

Commerce Utility Systeme können verteilt werden

[0127] Fig. 2A-Fig. 2E zeigen, wie das Distributed Commerce Utility **75** verteilt werden kann. Manche Administrations- und Unterstützungsfunktionen von Commerce Utility Systemen **90** können innerhalb eines verbraucherseitigen elektronischen Geräts **100** betrieben werden – oder gar in „aufgefächertem" Stil unter Beteiligung einer Vielzahl unterschiedlicher, untereinander kooperierender Geräte.

[0128] Wie vorstehend beschrieben, stellen die Geräte **100** jeweils eine geschützte Verarbeitungsumgebung **154** bereit, die manipulationssicher ist und einen sicheren Ort bereitstellt, an dem Administrations- und Unterstützungsabläufe ausgeführt werden können. Hierdurch kann ein elektronisches Gerät **100** im Heimbereich des Verbrauchers Vorgänge ausführen, die für andere Parteien wie etwa Rechteinhaber und Teilnehmer des elektronischen Handels vertrauenswürdig sind. Aufgrund der Vertrauenswürdigkeit und Geschütztheit der geschützten Verarbeitungsumgebung **154** können die Teile und Erweiterungen eines Commerce Utility Systems **90** oder sogar das gesamte Commerce Utility System innerhalb jeder oder einer beliebigen der geschützten Verarbeitungsumgebungen **154** und der betreffenden elektronischen Geräte im Gesamtsystem existieren.

[0129] Fig. 2A-Fig. 2E stellen die Gesamtfunktionen eines exemplarischen Commerce Utility Systems **90** dar, etwa am Beispiel eines Usage-Clearinghauses **300** in Form eines vierteiligen Puzzles.

[0130] Fig. 2A-Fig. 2E zeigen, dass diese Funktionen eines Commerce Utility Systems verschieden stark verteilt werden können. Beispielsweise:

• zeigt Fig. 2A ein Beispiel, in dem sämtliche Funktionen des Commerce Utility Systems **90** in einer sicheren Zentraleinrichtung ausgeführt werden.

• zeigt Fig. 2B ein Beispiel, in dem die meisten Funktionen des Commerce Utility Systems **90** in einer sicheren Zentraleinrichtung ausgeführt werden, einige Funktionen des Commerce Utility Systems jedoch innerhalb der geschützten Verarbeitungsumgebung **154** eines benutzerseitigen elektronischen Geräts **100** ausgeführt werden.

• zeigt Fig. 2C ein Beispiel, in dem einige der Funktionen des Commerce Utility Systems **90** in einer sicheren Zentraleinrichtung ausgeführt werden, die meisten der Funktionen des Commerce Utility Systems **90** jedoch innerhalb der geschützten Verarbeitungsumgebung **154** eines verbraucherseitigen elektronischen Geräts **100** ausgeführt werden.

• zeigt Fig. 2D ein Beispiel, in dem einige Funkti-

onen des Commerce Utility Systems **90** in einer sicheren Zentraleinrichtung ausgeführt werden, einige seiner Funktionen innerhalb der geschützten Verarbeitungsumgebung **154A** eines ersten benutzerseitigen elektronischen Geräts **100A** ausgeführt werden und einige seiner Funktionen innerhalb der geschützten Verarbeitungsumgebung **154B** eines zweiten benutzerseitigen elektronischen Geräts **100B** ausgeführt werden.

• zeigt Fig. 2E ein Beispiel, in dem keine der Funktionen des Commerce Utility Systems **90** in einer sicheren Zentraleinrichtung ausgeführt wird; einige seiner Funktionen innerhalb der geschützten Verarbeitungsumgebung **154(1)** eines ersten benutzerseitigen elektronischen Geräts **100(1)** ausgeführt werden, einige seiner Funktionen innerhalb der geschützten Verarbeitungsumgebung **154(2)** eines zweiten benutzerseitigen elektronischen Geräts **100(2)** ausgeführt werden , einige seiner Funktionen innerhalb der geschützten Verarbeitungsumgebung **154(3)** eines dritten benutzerseitigen elektronischen Geräts **100(3)** ausgeführt werden und einige seiner Funktionen innerhalb der geschützten Verarbeitungsumgebung **154(N)** eines N-ten benutzerseitigen elektronischen Geräts **100(N)** ausgeführt werden.

[0131] Alternativ oder zusätzlich können einige der Funktionen des Commerce Utility Systems **90** innerhalb des Netzwerks **150** verteilt werden – beispielsweise in der Ausrüstung, die für die Datenübertragung zwischen den Geräten **100** eingesetzt wird.

Verteilung mehrerer Administrations- und Unterstützungsfunktionen

[0132] Fig. 3A zeigt, wie mehrere Funktionen eines Commerce Utility Systems **90** oder Unterfunktionen in derselben geschützten Verarbeitungsumgebung **154** verteilt werden können.

[0133] Zum Beispiel:

• Die Funktion **200a** eines Finanz-Clearinghauses, die innerhalb der geschützten Verarbeitungsumgebung **154a** eines Verbrauchergeräts **100A** betrieben wird, kann gewisse Finanzclearing-Funktionen bereitstellen wie etwa das Auditing, das einige der durch ein zentralisiertes Finanz-Clearinghaus **200** ausgeführten Finanzclearing-Vorgänge ersetzen und/oder unterstützen kann.

• Die Funktion **300a** eines Usage-Clearinghauses, die innerhalb der geschützten Verarbeitungsumgebung **154a** eines Verbrauchergeräts **100A** betrieben wird, kann bestimmte auf Benutzungsdaten bezogene Clearing-Vorgänge ausführen wie beispielsweise die Kombination oder Analyse gewonnener Benutzungsdaten, um durch das Usage-Clearinghaus **300** ausgeführte Benutzungs-bezogene Clearing-Vorgänge zu ergänzen, zu ersetzen oder zu diesen Vorgänge hinzuzufügen.

[0134] Die geschützte Verarbeitungsumgebung **154a** von Gerät **100A** kann bestimmte Rechte- und Berechtigungs-bezogene Clearing-Vorgänge **400a**, bestimmte Vorgänge **500a** der zertifizierenden Behörde und bestimmte sichere Unterstützungsabläufe **600a** der Verzeichnis-Dienste jeweils am Verbraucher-Standort ausführen, um durch das Rechte- und Berechtigungs-Clearinghaus **400**, die zertifizierende Behörde **500** und sichere Verzeichnis-Dienste **600** ausgeführte Vorgänge zu ergänzen, zu ersetzen oder zu diesen Vorgänge hinzuzufügen.

[0135] Fig. 3B zeigt, dass weitere exemplarische elektronische Verbrauchergeräte **100(2)**, ..., **100N** (in diesem Fall Personalcomputer **124**) ggf. verschiedene Kombinationen aus Unterstützungs- oder Administrationsfunktionen lokal ausführen können (beispielsweise einige oder alle der durch die Transaktionsbehörde **700** ausgeführten Funktionen). Beispielsweise:

• können die Vorgänge innerhalb der geschützten Verarbeitungsumgebung **154(1)** auf einem teilweise verteilten und teilweise zentralisierten Finanz-Clearinghaus **200A**, einem teilweise verteilten und teilweise zentralisierten Usage-Clearinghaus **300A**, einem teilweise verteilten und teilweise zentralisierten Rechte- und Berechtigungs-Clearinghaus **400A**, einer teilweise verteilten und teilweise zentralisierten zertifizierenden Behörde **500A**, zentralisierten sicheren Verzeichnis-Diensten **600A**, und einer zentralisierten Transaktionsbehörde **700A** basieren;

• die Vorgänge innerhalb der geschützten Verarbeitungsumgebung **154(2)** können auf einem zentralisierten Finanz-Clearinghaus **200B**, einem teilweise verteilten und teilweise zentralisierten Usage-Clearinghaus **300B**, einem teilweise verteilten und teilweise zentralisierten Rechte- und Berechtigungs-Clearinghaus **400B**, einer zentralisierten zertifizierenden Behörde **500B**, zentralisierten sicheren Verzeichnis-Diensten **600B** und einer teilweise verteilten und teilweise zentralisierten Transaktionsbehörde **700B** basieren; und

• die Vorgänge innerhalb der geschützten Verarbeitungsumgebung **154(N)** können auf einem teilweise verteilten und teilweise zentralisierten Finanz-Clearinghaus **200N**, einem teilweise verteilten und teilweise zentralisierten Usage-Clearinghaus **300N**, einem teilweise verteilten und teilweise zentralisierten Rechte- und Berechtigungs-Clearinghaus **400N**, einer teilweise verteilten und teilweise zentralisierten zertifizierenden Behörde **500N**, teilweise verteilten und teilweise zentralisierten sicheren Verzeichnis-Diensten **600N** und einer teilweise verteilten und teilweise zentralisierten Transaktionsbehörde **700N** basieren.

[0136] Schreibt man die Idee verteilter Clearingdienste fort, so wäre es auch möglich, das Distributed Commerce Utility **75** gemäß Fig. 3C vollständig dergestalt zu verteilen, dass man sich weitgehend oder vollständig auf Vorgänge und Aktivitäten von Administrations- und Unterstützungsdiensten innerhalb der sicheren geschützten Verarbeitungsumgebungen **154** elektronischer Verbrauchergeräte **100** stützt. Auf diese Weise könnten die elektronischen Geräte **100** des Anwenders selbst in verteilter Form beliebige oder alle der folgenden Aufgaben ausführen: Finanz-, Usage- und Rechte- und Berechtigungs-Clearing sowie Zertifizierung, sichere Verzeichnis-Dienste und Transaktionsbehörden-Dienste. Eine solche „lokale" und/oder parallele und/oder verteilte Verarbeitung des Transaktionsclearings kann den Bedürfnissen individueller Verbraucher ggf. auf effizientere Weise Rechnung tragen. Auf diese Weise kann der Verbraucher beispielsweise Steuermechanismen beisteuern, mit denen er verhindern kann, dass sein elektronisches Gerät permanent bestimmte persönliche Daten ausgibt, mit denen er aber gleichzeitig dafür Sorge tragen kann, dass Rechteinhaber mit den wichtigsten, von ihnen benötigten Daten versorgt werden.

[0137] Die verteilten Anordnungen gemäß Fig. 2A-Fig. 2E und Fig. 3A-Fig. 3C schließen sich als Möglichkeiten der Bereitstellung eines zentralisierten Commerce Utility Systems **90** nicht gegenseitig aus. Vielmehr kann es von Vorteil sein, gemischte Anordnungen bereitzustellen, in denen einige Administrations- und Unterstützungsdienst-Funktionen (wie beispielsweise Mikro-Zahlungsaggregation, Benutzungsdaten-bezogene Datenschutzfunktionen und die Herausgabe bestimmter Zertifikate wie etwa durch Eltern, die für ihre Kinder Zertifikate herausgeben) stark verteilt sind, während andere Administrations- und Unterstützungsdienst-Funktionen (beispielsweise die Herausgabe wichtiger digitaler Zertifikate, die Wartung großer Datenbanken zur Unterstützung sicherer Verzeichnis-Dienste etc.) deutlich zentralisierter sind. Der Verteiltheitsgrad eines konkreten Administrations- und Unterstützungsdienstes, Clearinghauses oder einer Funktion/von konkreten Administrations- und Unterstützungsdiensten, Clearinghäusern oder Funktionen kann von verschiedenen sehr wichtigen Problemstellungen abhängen, wie etwa Effizienz, Vertrauenswürdigkeit, Skalierbarkeit, Anforderungen an die Ressourcen, Geschäftsmodelle und andere Faktoren. Ferner kann der Verteiltheitsgrad mehrere Hierarchieebenen beinhalten, die sich beispielsweise auf Teilmengen stützen, die durch bestimmte Geschäftsmodelle bestimmt werden, gefolgt von bestimmten untergeordneten Geschäftsmodellen oder beispielsweise geographischen Bereichen und/oder Bereichen eines leitenden Organs und/oder regionalen Bereichen.

[0138] Da ein bestimmtes elektronisches Gerät **100** an mehreren Aktivitäten teilnehmen kann, können sich seine unterschiedlichen Aktivitäten auf unterschiedliche Mischungen verteilter und zentralisierter Commerce Utility Systeme **90** stützen. Eine geschützte Verarbeitungsumgebung **154** kann sich beispielsweise bei einer Aktivität auf ein zentralisiertes Finanz-Clearinghaus **200** stützen, bei einer anderen Aktivität hingegen auf ein teilweise verteiltes und teilweise zentralisiertes Finanz-Clearinghaus **200** und bei noch einer weiteren Aktivität auf ein vollständig verteiltes Finanz-Clearinghaus **200**. Unterschiedliche Verteilungsgrade können für unterschiedliche Aktivitäten oder Geschäftsmodelle verwendet werden.

Netz aus Commerce Utility Systemen

[0139] Fig. 4 zeigt, dass Commerce Utility System **75** ein riesiges „Netz" verteilter, teilweise verteilter und/oder zentralisierter Commerce Utility Systeme **90** enthalten kann. Netzwerk **150** kann dazu verwendet werden, dieses Netz aus Commerce Utility Systemen **90** mit einer Anzahl verschiedener elektronischer Geräte **100** zu verbinden, die alle das Distributed Commerce Utility **75** teilen können. So kann das elektronische Netzwerk **150** beispielsweise mit Folgendem verbunden sein

- Set-Top-Boxes **106** und/oder Medienspielern **104**,
- Personalcomputern **124**,
- Workstations für Computergraphiken **126**,
- Multimedia-/Videospiel-Systemen **128** oder
- beliebigen anderen elektronischen Geräten **100** wie beispielsweise einem Gerät zur Fertigungssteuerung, Haushaltsgeräten, Ausrüstung zur Prozesssteuerung, Geräten für den Betrieb elektronischer Netzwerke und/oder anderen Geräten der Kommunikations-Infrastruktur, Großrechnern und/oder Minirechnern etc.

[0140] In diesem Beispiel kann ein und dasselbe Distributed Commerce Utility **75** unterschiedliche Arten von Aktivitäten einer Anzahl verschiedener Verbraucher, Autoren, Händler, Anbieter, Händler und anderer Personen unterstützen, wodurch das Distributed Commerce Utility **75** die verschiedensten elektronischen Aktivitäten unterstützen kann. Fig. 4 zeigt ferner, dass Commerce Utility Systeme **90** mit elektronischen Geräten **100** (und miteinander) dadurch kommunizieren können, dass sie zum Zweck der Sicherheit (z. B. Geheimhaltung, Echtheit und Integrität) untereinander elektronische „Container" **152** vom Typ wie in Ginter et al. offenbart, austauschen, die mit Hilfe von in geschützten Verarbeitungsumgebungen verarbeiteten Sicherheitsregeln und Steuermechanismen verwaltet werden.

Das Netz aus Commerce Utility Systemen kann praktisch grenzenlos sein

[0141] Fig. 4A zeigt, dass das Netz aus Commerce

Utility Systemen riesig oder grenzenlos sein kann. Netzwerk **150** kann tatsächlich ein nahtloses Netz sein, dass sich über die ganze Welt erstreckt und mehrere Millionen elektronischer Geräte mit beliebig vielen Commerce Utility Systemen **90** miteinander verbindet.

[0142] Das Netz aus Commerce Utility Systemen **90** kann eine sehr komplexe Netzanbindung mit einer Anzahl verschiedener Typen elektronischer Geräte bereitstellen und hierbei eine Anzahl verschiedener elektronischer Funktionen und Transaktionen ausführen. Wie vorstehend erwähnt, kann jedes der elektronischen Geräte **100** in die Lage versetzt werden, mit einem beliebigen der Commerce Utility Systeme **90** oder mit einem beliebigen anderen elektronischen Gerät zu kommunizieren. Dies ermöglicht eine maximale Effizienz und Flexibilität mit Hinblick auf Zuordnung verschiedener Commerce Utility Systeme zu verschiedenen elektronischen Transaktionen. Beispielsweise:

- Geographisch einander nahe gelegene Commerce Utility Systeme könnten am besten geeignet sein, um die für die Nachrichtenübermittlung in beiden Richtungen benötigte Zeit so gering wie möglich zu halten.
- In bestimmten Fällen könnten voneinander weitere entfernte Commerce Utility Systeme für eine effiziente Abwicklung bestimmter spezialisierter Transaktionen besser ausgestattet sein.
- Öffentliche Bestimmungen könnten überdies zumindest teilweise über eine Bevorzugung bestimmter Commerce Utility Systeme gegenüber anderen verfügen (beispielsweise könnte eine japanische Kundin in einen Rechtskonflikt geraten, wenn sie versucht, ein Finanz-Clearinghaus **200** auf den Cayman-Inseln zu verwenden, oder Einwohner von New Jersey könnten gesetzlich verpflichtet werden, mit einem Finanz-Clearinghaus **200** zusammen zu arbeiten, das die Umsatzsteuer an die Finanzbehörden von New Jersey meldet).
- Verschiedene konkurrierende Commerce Utility Systeme werden wahrscheinlich von verschiedenen Parteien angeboten werden, und diese verschiedenen Systeme würden das Netz bevölkern, das das Distributed Commerce Utility **75** beinhaltet. Die Interoperabilität zwischen solchen Systemen und/oder ihren Knoten ist wichtig für die Effizienz und die Ermöglichung einer Umnutzbarkeit von Ressourcen des elektronischen Handels.

Rechteinhaber und Anbieter können zwischen Commerce Utility Systemen wählen

[0143] Fig. 5 zeigt, wie Rechteinhaber zwischen verschiedenen Commerce Utility Systemen **90** wählen können. In diesem Beispiel betreibt Bob ein erstes Usage-Clearinghaus **300a**, Alice betreibt ein zweites Usage-Clearinghaus **300b** und Helen betreibt ein drittes Usage-Clearinghaus **300c**. Diese verschiedenen Usage-Clearing-Dienstleister können miteinander in qualitativer und/oder preislicher Hinsicht konkurrieren, oder sie können einander ergänzen (beispielsweise indem sie sich auf unterschiedliche Transaktionen spezialisieren).

[0144] Da das elektronische Netzwerk **150** elektronische Geräte **100** mit vielen verschiedenen Commerce Utility Systemen **90** verbinden kann, können Rechteinhaber an einer digitalen Eigenschaft, die die Verbraucher benutzen, zwischen verschiedenen Commerce Utility Systemen wählen. Anbieter von Inhalten und Rechteinhaber können bestimmte Commerce Utility Systeme **90** (oder Gruppen aus diesen) bevollmächtigen, verschiedene Aspekte von Transaktionen abzuwickeln. Beispielsweise:

- Ein Computersoftware-Händler könnte darüber verfügen, dass ein Personalcomputer **124** Messdaten **116a** an Helens Usage-Clearinghaus **300c** sendet, um die Benutzung der Computersoftware oder anderer Aktivitäten des Personalcomputers zu überwachen.
- Ein Rechteinhaber am Videoprogramm **102a** könnte darüber verfügen, dass die Set-Top-Box **106** Messdaten **116** über das Video an Alices Usage-Clearinghaus sendet.
- Ein Anbieter von Multimedia-Inhalten könnte darüber verfügen, dass Bobs Usage-Clearinghaus **300a** zur Verarbeitung der vom Multimedia-Player **128** generierten Benutzungsdaten **116c** verwendet wird.

[0145] In einigen Fällen können bestimmte Verbraucher **95** auch auf die Vorausbestimmung konkreter, von ihnen bevorzugter Clearinghäuser oder anderer Commerce Utility Systeme **90** Einfluss nehmen. Fig. 5 illustriert die Wahl durch den Anbieter (und/oder den Verbraucher) anhand eines Polizisten, der den Messdatenverkehr zu ausgewählten Usage-Clearinghäusern **300** lenkt (elektronische Steuermechanismen wie in der vorliegenden Schrift und in Ginter et al. beschrieben wären vorzugsweise der Mechanismus, der den Datenverkehr tatsächlich lenkt).

[0146] Ein Anbieter von Inhalten oder Rechteinhaber könnte einen Verbraucher **95** mit der Möglichkeit ausstatten, aus einer Gruppe Commerce Utility Systeme **90** (und/oder Anbieter von Commerce Utility Systemen **90**) zu wählen, mit denen der Anbieter von Inhalten/Rechteinhaber arbeiten möchte. Zum Beispiel:

- Ein Fernsehstudio könnte bestimmte individuelle Commerce Utility Systeme **90** oder Klassen aus diesen dazu bevollmächtigen, Transaktionen mit Hinblick auf seine Fernsehprogramme abzuwickeln und/oder es kann veranlassen, dass individuelle Commerce Utility Systeme **90** oder Klassen aus diesen seine Transaktionen nicht abwickeln.

• Bestimmte Commerce Utility Systeme **90** können Anforderungen oder Standards für individuelle Anbieter und/oder Verbraucher **95** (oder Klassen aus diesen) festlegen.
• Teilnehmer der Wertkette könnten rechtliche Vereinbarungen und/oder Geschäftsbeziehungen mit verschiedenen Commerce Utility Systemen **90** abschließen.

Commerce Utility Systeme können zusammenarbeiten

[0147] Fig. 6 zeigt, dass verschiedene Commerce Utility Systeme **90** zusammenarbeiten können, um verschiedene Arten von Vorgängen zu unterstützen. In diesem Beispiel:
• können das Usage-Clearinghaus **300a**, das Rechte- und Berechtigungs-Clearinghaus **400a**, die zertifizierende Behörde **500a**, und das Finanz-Clearinghaus **200a** (links in der Zeichnung) dazu verwendet werden, einen bestimmten Vorgang durch Set-Top-Box **106** und Fernseher **102** zu unterstützen.
• Dasselbe Finanz-Clearinghaus **200a**, jedoch ein anderes Usage-Clearinghaus **300b**, eine andere zertifizierende Behörde **500b** und ein anderes Rechte- und Berechtigungs-Clearinghaus **400b** (oben in der Zeichnung) könnte dazu verwendet werden, bestimmte Aktivitäten am Personalcomputer **124** zu unterstützen.
• Ein anderes Finanz-Clearinghaus **200c**, eine andere zertifizierende Behörde **500c** und ein anderes Usage-Clearinghaus **300c**, jedoch dasselbe Rechte- und Berechtigungs-Clearinghaus **400b** (rechts in der Zeichnung) könnte dazu verwendet werden, elektronische Aktivitäten des Multimedia-Systems **128** zu unterstützen.
• Eine weitere Kombination aus Commerce Utility Systemen (in diesem Beispiel Usage-Clearinghaus **300c**, Finanz-Clearinghaus **200d**, Rechte- und Berechtigungs-Clearinghaus **400c** und zertifizierende Behörde **500a** im unteren Bereich der Zeichnung) könnte dazu verwendet werden, Audio-Anlage **130** zu unterstützen.

[0148] Dieses Beispiel zeigt, dass verschiedene Commerce Utility Systeme **90** kombiniert betrieben werden können, und dass verschiedene Kombinationen aus Commerce Utility Systemen dazu verwendet werden könnten, verschiedene elektronische Transaktionen zu unterstützen.

Administrations- und Unterstützungsdienst-Funktionen können innerhalb universeller Commerce Utility Systeme für eine verbesserte Effizienz oder Benutzungsfreundlichkeit kombiniert werden

[0149] Fig. 7 zeigt, dass verschiedene Administrations- und Unterstützungsdienst-Funktionen oder -unterfunktionen spezialisierter Commerce Utility Systeme **90** in universelleren oder multifunktionalen Commerce Utility Systemen **90** zusammengefasst werden können, um Benutzungsfreundlichkeit und Effizienz zu maximieren oder ein anderes Ziel zu erreichen. Zum Beispiel:
• Bob kann ein integriertes oder kombiniertes Commerce Utility System **90a** betreiben, das die Funktion eines Finanz-Clearinghauses **200a**, einer zertifizierenden Behörde **500a** und eines Usage-Clearinghauses **300a** bereitstellt.
• Anne kann ein integriertes oder kombiniertes Commerce Utility System **90b** betreiben, das die Funktion eines Finanz-Clearinghauses **200b**, eines Rechte- und Berechtigungs-Clearinghauses **400b** und einer Transaktionsbehörde **700b** bereitstellt.
• Helen kann ein integriertes oder kombiniertes Commerce Utility System **90c** betreiben, das die Funktion eines Rechte- und Berechtigungs-Clearinghauses **400c** und einer zertifizierenden Behörde **500c** bereitstellt.
• Roger kann ein integriertes oder kombiniertes Commerce Utility System **90d** betreiben, das sichere Verzeichnis-Dienste **600d**, Usage-Clearinghaus-Dienste **300d**, Finanz-Clearinghaus-Dienste **200d** und ein Rechte- und Berechtigungs-Clearinghaus **400d** bereitstellt.

[0150] Ein Verbraucher, der elektronische Geräte **100** betreibt, kann auf jedes oder alle dieser verschiedenen Commerce Utility Systeme **90** oder auf Kombinationen aus diesen zugreifen. Beispielsweise könnte Set-Top-Box **106** Rechte und Berechtigungen und Zertifikate von Helens Commerce Utility System **90c** erwerben, gleichzeitig jedoch für Finanz-Clearing und Benutzungsanalyse auf das Commerce Utility System **90a** von Bob zurückgreifen.

[0151] Ein Commerce Utility System **90** kann eine beliebige Kombination aus Administrations- und Unterstützungsfunktionen oder Unterfunktionen bereitstellen, wie zur Ausführung der in bestimmten Geschäftsmodellen erforderlichen Vorgänge erforderlich, und maximale Effizienz und/oder Benutzungsfreundlichkeit bereitzustellen. Beispielsweise könnte Annes Commerce Utility System **90(2)** nur eine spezialisierte Teilmenge einer Finanz-Clearinghaus-Funktion bereitstellen.

[0152] Fig. 7A illustriert an einem weiteren Beispiel, wie Commerce Utility Systeme **90** eine große Bandbreite an verschiedenen Kombinationen oder Unterkombinationen aus Administrations- und Unterstützungsfunktionen ermöglichen können. In diesem Schaubild der Fig. 7A ist jede der verschiedenen Administrations- und Unterstützungsdienst-Funktionen (zu Illustrationszwecken) mit jeweils einer eigenen Bauklotz-Form dargestellt:
• Finanzclearing-Funktionen **200** sind als quadratische Klötze dargestellt,

- Usage-Clearing-Funktionen **300** sind als halbkreisförmige Klötze dargestellt,
- Funktionen des Rechte- und Berechtigungs-Clearing **400** sind als rechteckige Klötze dargestellt,
- Funktionen der zertifizierenden Behörde **500** sind als dreieckige Klötze dargestellt,
- Funktionen sicherer Verzeichnis-Dienste **600** sind als Tunnel-Klötze dargestellt, und
- Funktionen der Transaktionsbehörde **700** sind als Zylinder dargestellt.

[0153] Verbraucher- und benutzerseitige Geräte **100** sind im Schaubild als aufrecht stehende rechteckige Säulen dargestellt. Das elektronische Netzwerk **150** ist als Straße dargestellt, die die verschiedenen Commerce Utility Systeme miteinander und mit den verbraucherseitigen elektronischen Geräten **100** verbindet. Über dieses elektronische Netzwerk bzw. die „Datenautobahn" **150** zwischen verschiedenen elektronischen Installationen können elektronische digitale Container **152** befördert werden.

[0154] Fig. 7A illustriert nur einige der vielen möglichen Kombinationen von Administrations- und Unterstützungsdiensten, die Verwendung finden könnten. Zum Beispiel:

- Links oben stellt ein Commerce Utility System **90A** mindestens einige Finanzclearing-Funktionen **200a**, mindestens einige Funktionen des Rechte- und Berechtigungs-Clearings **400a** und mindestens einige Zertifizierungsfunktionen **500a** bereit. Dieser Typ eines übergeordneten elektronischen Commerce Utility Systems **90A** könnte beispielsweise die Aufgabe haben, Rechte im Namen der Rechteinhaber zu verwalten und zu erteilen sowie Zahlungen auf Grundlage dieser Rechte abzuwickeln.
- Das Commerce Utility System **90D** gleich rechts neben Installation **90A** enthält Finanzclearing-Dienste **200d** und Transaktionsbehörden-Dienste **700a**. Es könnte besonders sinnvoll sein, beispielsweise eine übergeordnete komplexe, mehrere Schritte enthaltene Transaktion zu prüfen und/oder zu verwalten, während gleichzeitig sichergestellt wird, dass die entsprechenden Parteien der Transaktion bezahlt werden.
- In der Mitte weiter unten im Schaubild befindet sich ein Commerce Utility System **90B** mit Finanz-Clearing-Funktionen **200f** und Usage-Clearing-Funktionen **300c**. Dieses Commerce Utility System **90B** könnte besonders sinnvoll sein beispielsweise zur Abwicklung von Zahlungen und anderen finanziellen Vorgängen in Bezug auf Transaktionen elektronischer Benutzung und auch zur Bereitstellung von Audit- und Berichtdiensten auf der Grundlage elektronischer Benutzung.
- Das Commerce Utility System **90C** in der unteren Mitte der Zeichnung kombiniert Dienste einer zertifizierenden Behörde **500** mit Usage-Clearing-Diensten **300f**. Es könnte besonders sinnvoll sein, digitale Zertifikate herauszugeben und hiernach die Benutzung solcher Zertifikate mitzuverfolgen (beispielsweise, um Risiken, eine potentielle Haftung, Versicherungskosten etc. zu bewerten).

[0155] Die verschiedenen in Fig. 7A gezeigten Beispiele dienen lediglich der Veranschaulichung. In Abhängigkeit von den Geschäftszielen, der Benutzungsfreundlichkeit und anderen Faktoren sind auch andere Kombinationen möglich oder wahrscheinlich.

Hierarchien eines Commerce Utility Systems

[0156] Fig. 8A zeigt, dass Commerce Utility Systeme **90** oder -Funktionen hierarchisch angeordnet werden können. Beispielsweise kann ein übergeordnetes Finanz-Clearinghaus (oder ein anderes übergeordnetes Clearinghaus) **200(N)** die Vorgänge vieler anderer untergeordneter Finanz-Clearinghäuser (oder anderer untergeordneter Clearinghäuser) **200(1)**, **200(2)**, ... überwachen und/oder für deren Vorgänge verantwortlich sein. Im Beispiel von Fig. 8A könnte ein elektronisches Verbrauchergerät **100** mit einem Clearinghaus **200(1)** interagieren, das seinerseits wieder mit einem weiteren Clearinghaus **200(2)** etc. interagieren könnte. Diese Hierarchie eines Administrations- und Unterstützungsdienstes könnte in gewisser Hinsicht mit einer Befehlskette in einem großen Unternehmen oder beim Militär verglichen werden, wobei einige Clearinghäuser gegenüber anderen Clearinghäusern Vollmachten, Kontrolle und/oder Überwachungsaufgaben ausüben und/oder delegieren.

[0157] Fig. 8B zeigt eine weitere exemplarische Hierarchie eines Administrations- und Unterstützungsdienstes. In diesem Beispiel delegieren einige zentralisierte übergeordnete Clearinghäuser und/oder andere Commerce Utility Systeme **90** ihre Arbeitsverantwortung teilweise oder ganz an andere Commerce Utility Systeme **90**. In diesem konkreten Beispiel können Organisationen wie Unternehmen, gemeinnützige Gruppen oder ähnliches über ihre eigenen Commerce Utility Systeme **156** verfügen. Bestimmte Aktivitäten des elektronischen Handels oder andere Aktivitäten (beispielsweise der Unterhaltungsindustrie) könnten über ihre eigenen vertikal spezialisierten Commerce Utility Systeme **158** verfügen. Bestimmte geographische, territoriale oder unter eine bestimmte Gerichtsbarkeit fallende Gruppen (beispielsweise sämtliche Käufer bestimmter Produkte innerhalb des Bundesstaats Wisconsin) können über ihre eigenen, auf das Territorium/die Gerichtsbarkeit spezialisierten Commerce Utility Systeme **160** verfügen. Die hierarchisch niedriger angeordneten Commerce Utility Systeme **156**, **158**, **160** können wiederum Vollmachten oder Verantwortungen an be-

stimmte Verbraucher, Organisationen oder andere Einheiten weiterdelegieren.

[0158] In einem Anordnungsbeispiel können solche Commerce Utility Systeme **90**, an die bestimmte Vollmachten delegiert wurden, praktisch sämtliche tatsächlich anfallende Unterstützungsarbeit ausführen, gleichzeitig jedoch die mehr übergreifenden Commerce Utility Systeme **90** mittels Berichterstattung oder auf anderem Wege auf dem Stand halten. In einer weiteren Anordnung sind die übergreifenden Commerce Utility Systeme **90** an den alltäglichen Aktivitäten der Commerce Utility Systeme, an die sie Arbeit delegiert haben, in keiner Weise beteiligt. In einem weiteren Anordnungsbeispiel erledigen die spezialisierteren Commerce Utility Systeme einen Teil der Arbeit und die mehr übergreifenden Commerce Utility Systeme einen anderen Teil der Arbeit. Die konkrete, in einem konkreten Szenario angewandte Arbeitsteilung und Teilung von Vollmachten kann weithin von Faktoren wie Effizienz, Vertrauenswürdigkeit, Verfügbarkeit von Ressourcen, der Art der zu verwaltenden Transaktionen und verschiedenen anderen Faktoren abhängen. Die Übertragung von Vollmachten für Clearingaktivitäten kann sich auf Teilaufgaben beziehen (beispielsweise Übertragung von Verantwortungen der Usage Aggregation, jedoch nicht der Finanz- oder Rechteverwaltung), und sie kann mit Peer-to-Peer-basierter Verarbeitung vereinbar sein (indem beispielsweise einige Funktionen in verbraucherseitigen elektronischen Geräten untergebracht werden, während einige wichtigere Funktionen zentralisiert ausgeführt werden).

Multifunktionale Commerce Utility Systeme können hierarchisch oder Peer-to-Peer-basiert organisiert werden

[0159] Fig. 9 zeigt eine weitere komplexere Umgebung eines Commerce Utility Systems mit Elementen sowohl einer hierarchischen Befehlskette als auch mit hohem Kooperationsgrad in horizontaler Ausrichtung zwischen verschiedenen multifunktionalen Commerce Utility Systemen **90**. In diesem Beispiel existieren fünf verschiedene Verantwortungsebenen mit einem übergeordneten oder übergreifenden Commerce Utility System **90(1)** (beispielsweise ein Finanz-Clearinghaus **200**) auf Ebene **1**, das mit den meisten Vollmachten ausgestattet ist, und zusätzlichen Commerce Utility Systemen auf Ebenen **2**, **3**, **4**, und **5**, die weniger Vollmachten, Autorität, Kontrollaufgaben, ein kleineres Aufgabengebiet und/oder weniger Verantwortung haben als jenes der jeweils nächsthöheren Ebene. Fig. 9 zeigt ferner, dass verschiedene Commerce Utility Systeme derselben Ebene verschiedene Funktionen, Aufgabengebiete und/oder Verantwortungsbereiche haben können. Beispielsweise:

- ein Commerce Utility System **90(2)(1)** kann ein Commerce Utility System des „Typs A" sein,
- Commerce Utility System **90(2)(2)** könnte ein Commerce Utility System des „Typs B" sein, und
- Commerce Utility System **90(2)(3)** könnte ein Commerce Utility System des „Typs C" sein.

[0160] Auf der nächsttieferen Ebene könnten die Commerce Utility Systeme dem Typ A angehören (wie etwa **90(3)(1)** und **90(3)(2)**), sie könnten dem Typ B angehören (wie etwa **90(3)(4)**), sie könnten dem Typ C angehören (wie etwa **90(3)(5)**, **90(3)(6)**), oder sie könnten Mischformen darstellen wie etwa Commerce Utility System **90(3)(3)**, das eine Mischform ist und Funktionen des Typs A und des Typs B erfüllt.

[0161] Fig. 9 zeigt ferner, dass zusätzliche Clearinghäuser auf den Ebenen **4** und **5** Subtypen wie auch Typen aufweisen können. In der Umgebung eines Finanz-Clearinghauses **200** könnte Typ A beispielsweise für Verbraucherkredite, Typ B für elektronische Checks, und Typ C für Handelskredite verantwortlich sein. Eine andere Aufgabenverteilung könnte Clearing für Visa (Typ A), Mastercard (Typ B) und American Express (Typ C) sein. Ein Clearinghaus vom Typ A/B würde dann sowohl das Clearing von Verbraucherkrediten als auch von elektronischen Schecks übertragen bekommen. Ein Subtyp I vom Typ B könnte für elektronische Schecks im Handel verantwortlich sein. Ein Subtyp I vom Typ C könnte für Transaktionen mit Kreditkarten im Handel zur Anwendung kommen, und Subtyp III für Zahlungsanweisungen. Eine Motivation für die Einrichtung mehrerer Instanzen könnten Gerichtsbarkeitsgrenzen (beispielsweise Frankreich, Deutschland, New York und Alabama) und/oder vertragliche Übereinkommen (beispielsweise Übertragung von Verantwortung für erhöhte Kreditrisiken, Kleineinkäufe, sehr große Transaktionen etc.) darstellen. Die Peer-to-Peer-Dimension könnte die Koordination einer Gesamt-Transaktion (beispielsweise zwischen dem Clearinghaus eines Einzelhändlers und jenem eines großen Handelsplayers) erforderlich machen.

[0162] Ein Rechte- und Berechtigungs-Clearinghaus **400** könnte unter Inhalts-Typen (z. B. Spielfilme; Wissenschaft, Technik und Medizin und Software) ausscheren. Subtyp A könnte neue Spielfilme, Oldies und künstlerische Filme umfassen; Subtyp B könnte für Zeitschriften und Lehrbücher eingesetzt werden und Typ C könnte für Spiele, Büro und Bildungsinhalte verantwortlich sein. Peer-to-peer-basierter Datenverkehr zwischen Clearinghäusern könnte Berechtigungen für Multimedia-Vorführungen umfassen (beispielsweise könnte eine Multimedia-Vorführung Berechtigungen in einem Clearinghaus abspeichern, das mit anderen Clearinghäusern kommuniziert, um sicherzustellen, dass jeweils die aktuellen Berechtigungen verteilt werden).

Einige Beispiele für Commerce Utility Systeme

[0163] Wie vorangehend beschrieben, sind Commerce Utility Systeme **90** verallgemeinert und programmierbar und können hierdurch eine Mischung verschiedener Unterstützungs- und Administrations-Funktionen bereitstellen, um den Anforderungen der betreffenden Transaktion gerecht zu werden. Somit können viele oder die meisten der Commerce Utility Systeme **90** so, wie sie schließlich tatsächlich implementiert werden, eine Reihe verschiedener Unterstützungs- und Administrations-Funktionen dergestalt bereitstellen, dass es schwierig wird, die Implementierung als eine bestimmte „Art" eines Commerce Utility Systems in Abgrenzung gegenüber einer anderen einzustufen.

[0164] Dennoch sind bestimmte Typen idealisierter spezialisierter Commerce Utility Systeme **90** für die unterschiedlichsten Modelle, Transaktionen und Anwendungen besonders sinnvoll. Es ist hilfreich und sinnvoll, einige der Merkmale dieser „reinen" Commerce Utility Systeme verschiedener Typen zu beschreiben, ohne hierbei zu vergessen, dass in den tatsächlichen Implementierungen Funktionen oder Teilfunktionen mehrerer dieser idealisierter Modelle in gemischter Form auftreten können. Nachstehend werden kurze Vignetten einige der Merkmale solcher „reinen" idealisierten Commerce Utility Systeme vorgestellt.

Finanz-Clearinghaus **200**

[0165] Fig. 10 zeigt ein ausführliches Beispiel für ein Finanz-Clearinghaus **200**. Finanz-Clearinghaus **200** wickelt Zahlungen ab und stellt damit sicher, dass jene, die Werte bereitstellen, gerecht entschädigt werden. Finanz-Clearinghaus **200** kann für das Erfüllen dieser Aufgabe sicher mit anderen Commerce Utility Systemen **90** zusammenarbeiten.

[0166] In diesem Beispiel kann Finanz-Clearinghaus **200** mit der geschützten Verarbeitungsumgebung **154** eines Geräts über das elektronische Netzwerk **150** auf sichere Weise unter Verwendung der elektronischen Container **152** vom Typ wie beispielsweise in der Patentschrift von Ginter et al. in Verbindung mit den **Fig.** 5A und 5B beschrieben kommunizieren. Das Finanz-Clearinghaus **200** kann von der geschützten Verarbeitungsumgebung **154** in diesen sicheren Containern **152** Zahlungsinformationen **202** erhalten und elektronisch oder anderweitig mit verschiedenen Banking-, Kreditkarten- oder anderen Geldinstituten interagieren, um sicherzustellen, dass die Zahlung ordnungsgemäß erfolgt.

[0167] Finanz-Clearinghaus **200** kann beispielsweise mit der Bank eines Verbrauchers **206a**, der Bank eines Anbieters **206b** und dem Kreditkartenunternehmen eines Verbrauchers **206c** interagieren. Beispielsweise kann Finanz-Clearinghaus **200** einen Betrag von der Bank des Verbrauchers **206a** einziehen und einen Betrag bei der Bank des Rechteinhabers **206b** gutschreiben, womit der Verbraucher dafür bezahlt hat, dass er sich einen Spielfilm, ein Fernsehprogramm oder andere Inhalte ansieht. Zusätzlich oder abwechselnd kann Finanz-Clearinghaus **200** mit dem Kreditkartenunternehmen **206c** des Verbrauchers interagieren, um Kreditchecks anzufordern, Kreditbewilligungen zu erwerben, Zahlungen auszulösen oder ähnliches.

[0168] Finanz-Clearinghaus **200** kann für die Verbraucher **95** Zahlungsbestätigungen **204** bereitstellen, beispielsweise durch Übermittlung der Bestätigungen an Gerät **100** in einem sicheren elektronischen Container **152b**, um die Vertraulichkeit der in der Bestätigung enthaltenen Informationen zu wahren. In diesem Beispiel können sich Verbraucher **95** die Bestätigungen **204** über die geschützte Verarbeitungsumgebung **154** ihres Geräts **100** anzeigen lassen und sind überdies in der Lage, diese zu buchhalterischen Zwecken auszudrucken oder abzuspeichern.

[0169] In einem Beispiel könnte der durch die geschützte Verarbeitungsumgebung **154** bereitgestellte Zahlungsmechanismus **118** die Gestalt einer elektronischen Geldbörse haben, die elektronisches Geld zur Bezahlung elektronischer Dienstleistungen oder Inhalte ausgibt. Diese elektronische Geldbörse kann Geld in digitaler Form enthalten. Verbraucher **95** können digitales Geld für beliebige Dinge ausgeben. Wenn die elektronische Geldbörse leer ist, können die Verbraucher **95** das Finanz-Clearinghaus **200** anweisen, die Geldbörse wieder aufzufüllen, indem sie das Finanz-Clearinghaus dazu ermächtigen, den Betrag vom Verbraucherkonto ihrer Bank **206a** einzuziehen. Finanz-Clearinghaus **200** kann Zahlungsvorgänge mit elektronischem Geld abwickeln, eine automatische Wiederauffüllung der elektronischen Geldbörse veranlassen (beispielsweise auf Grundlage einer vom Verbraucher vorab erteilten Vollmacht), wenn die Verbraucher alle ihrer vormaligen Inhalte verbraucht haben und für die Verbraucher detaillierte Berichte und Zahlungsbestätigungen **204** bereitstellen, die Auskunft darüber geben, wie diese ihr elektronisches Geld ausgegeben haben.

Usage-Clearinghaus **300**

[0170] Fig. 11 zeigt ein Beispiel für ein Usage-Clearinghaus **300**. Usage-Clearinghaus **300** empfängt in diesem Beispiel Benutzungsdaten 302 vom Benutzungszähler **116**, analysiert die Benutzungsdaten und stellt auf der Grundlage der von ihm durchgeführten Analyse Berichte bereit. Usage-Clearinghaus **300** kann für das Erfüllen dieser Aufgaben sicher mit anderen Commerce Utility Systemen **90** zusammenarbeiten.

[0171] Usage-Clearinghaus **300** kann beispielsweise einen detaillierten Bericht **304a** über alle Spielfilme, Fernsehprogramme und anderes Material, das die Verbraucher sich im vergangenen Monat angesehen haben, an die Verbraucher **95** senden. Der Datenaustausch zwischen der geschützten Verarbeitungsumgebung **154** und dem Usage-Clearinghaus **300** kann in Form von sicheren Containern **152** stattfinden. Wie in der Offenbarung des Patents von Ginter et al. beschrieben, können Benutzungszähler **116** die Benutzung auf der Grundlage verschiedener Faktoren messen und Einstellungen von äußert detaillierten Aufzeichnungen bis hin zur kompletten Abschaltung ermöglichen. Die Verbraucher könnten im Bedarfsfall den detaillierten Benutzungsbericht **304a** von ihrem Fernseher **102** anzeigen lassen.

[0172] Usage-Clearinghaus **300** kann an andere Clearinghäuser über die Fernsehgewohnheiten des Verbrauchers unter Wahrung des Datenschutzes gegenüber dem Verbraucher Bericht erstatten. Diese Berichte können auch mittels sicherer Container **152** übermittelt werden. Usage-Clearinghaus **300** könnte für Werbetreibende **306** beispielsweise einen Kurzbericht **304b** bereitstellen, in dem keine Angaben über die Identität des Verbrauchers enthalten sind, der aber den Werbetreibenden mit wertvollen Informationen über die Fernsehgewohnheiten des Verbrauchers versorgt. Usage-Clearinghaus **300** könnte mit Zustimmung des Verbrauchers jedoch auch einen detaillierteren Bericht bereitstellen, in dem die Identität des Verbrauchers gegenüber dem Werbetreibenden **306** oder anderen vorgegebenen Personen offen gelegt wird. Im Gegenzug könnte der Verbraucher **95** Anreize erhalten wie beispielsweise Preisnachlässe, Geld, kostenlose Spielfilme oder andere Gegenleistungen.

[0173] Usage-Clearinghaus **300** kann auch Berichte **304c** an Rechteinhaber **308** ausgeben wie an den Produzenten oder Regisseur der von Verbraucher **95** angesehenen Videosendung **102a**. Mit diesen Berichten können die Rechteinhaber überprüfen, wer sich ihr Sendungsmaterial und andere Werke angesehen hat. Dies kann sehr nützlich sein, wenn es darum geht sicherzustellen, dass der Verbraucher auch tatsächlich bezahlt oder darum, dem Verbraucher anderes ähnliches Sendungsmaterial zukommen zu lassen, an dem er interessiert sein könnte.

[0174] Das Usage-Clearinghaus **300** könnte auch Berichte **304d** an ein Ratingunternehmen **310** senden, um eine automatisches Rating der Beliebtheit eines bestimmten Sendungsmaterials zu ermöglichen. Usage-Clearinghaus **300** könnte zum Zweck der wissenschaftlichen Forschung, Marktforschung oder einer anderen Form der Forschung auch Berichte an andere Marktforscher **312** senden.

Rechte- und Berechtigungs-Clearinghaus **400**

[0175] Fig. 12 zeigt ein Beispiel für ein Rechte- und Berechtigungs-Clearinghaus **400**. Das Rechte- und Berechtigungs-Clearinghaus **400** speichert und verteilt elektronische Berechtigungen **404** (in diesen Zeichnungen als Ampel dargestellt). Berechtigungen **404** erteilen und verweigern Berechtigungen und definieren überdies Konsequenzen. Bei der Erfüllung dieser Aufgaben kann das Rechte- und Berechtigungs-Clearinghaus **400** mit anderen Commerce Utility Systemen **90** zusammenarbeiten.

[0176] In diesem Beispiel kann das Rechte- und Berechtigungs-Clearinghaus **400** als zentralisiertes „Repository" oder Clearinghaus für Rechte an digitalen Inhalten fungieren. Rundfunkanstalten, Autoren und andere Ersteller von Inhalten und Rechteinhaber können beispielsweise im Rechte- und Berechtigungs-Clearinghaus **400** in Form elektronischer „Regelsätze" Berechtigungen registrieren. Mit diesen Berechtigungen kann festgelegt werden, welcher Verbraucher mit digitalen Eigenschaften was tun kann und was nicht, unter welchen Bedingungen die Berechtigungen ausgeübt werden können und mit welchen Konsequenzen. Das Rechte- und Berechtigungs-Clearinghaus **400** kann auf Anforderungen **402** der geschützten Verarbeitungsumgebung **154** des elektronischen Geräts mit der Erteilung von Berechtigungen (Regelsätze) **188** reagieren.

[0177] Angenommen, Verbraucher **95** möchten sich beispielsweise am Fernseher **102** ein Konzert oder einen Boxkampf ansehen. Sie können per Fernbedienung **108** das Recht anfordern, eine bestimmte Sendung sehen zu dürfen. Die geschützte Verarbeitungsumgebung **154** kann automatisch das Rechte- und Berechtigungs-Clearinghaus **400** über das elektronische Netzwerk **150** kontaktieren und eine elektronische Anforderung **402** absenden. Das Rechte- und Berechtigungs-Clearinghaus **400** kann die Anfrage in seiner Bibliothek oder seinem Repository „nachschlagen", um festzustellen, ob es die erforderliche Berechtigung **404b** vom Rechteinhaber **400** an der Sendung erhalten hat (und bevollmächtigt ist, diese zu erteilen). Hiernach kann es die angeforderte Berechtigung **188** an die geschützte Verarbeitungsumgebung **154** schicken.

[0178] Berechtigung **188** könnte beispielsweise den Verbrauchern die einmalige Betrachtung des Konzerts oder Boxkampfes ermöglichen und mit Hilfe des Kopierschutzmechanismus **120** dessen Kopie verbieten. Berechtigung **188** kann auch (bzw. zusätzlich) den Preis für die Betrachtung des Sendung bestimmen (beispielsweise dass $ 5,95 von der elektronischen Geldbörse des Verbrauchers eingezogen werden). Gerät **100** kann die Verbraucher **95** fragen, ob sie $ 5,95 bezahlen möchten, um die Sendung zu sehen. Antworten sie mit „Ja" (beispielsweise mittels

Fernbedienung **108**), so kann Gerät **100** den Betrag von der elektronischen Geldbörse des Verbrauchers automatisch einziehen und die Sendung „freigeben", woraufhin die Verbraucher sie sich ansehen können.

[0179] Das Rechte- und Berechtigungs-Clearinghaus **400** kann Berechtigungen **188** in einem sicheren Container **152b** bereitstellen, der optional auch die durch die Berechtigungen gesteuerten Informationen enthalten kann, oder Berechtigung **188** kann zu einem anderen Zeitpunkt und über einen anderen Pfad als jenem eintreffen, auf dem die Sendung oder andere Inhalte zum Gerät **100** gelangen. Beispielsweise könnten die Berechtigungen über Netzwerk **150** verschickt werden, während die dazugehörige Sendung direkt per Satellit **112** oder über einen anderen Pfad wie Kabel-TV-Netzwerk **114** (siehe Fig. 1) übertragen werden kann.

[0180] Das Rechte- und Berechtigungs-Clearinghaus **400** kann auch Berichte **406** für Rechteinhaber oder andere Personen erstellen, in denen genannt wird, welche Berechtigungen erteilt oder verweigert wurden. Der Autor eines Buchs oder Videos könnte beispielsweise unter Beachtung des Verbraucher-Datenschutzes in der Lage sein, zu erfahren, wie viele Personen genau das Recht angefordert haben, Auszüge aus seinem bzw. ihrem Werk zu veröffentlichen. Solche Berichte können die durch das Usage-Clearinghaus **300** bereitgestellten Berichte ergänzen.

Zertifizierende Behörde **500**

[0181] Fig. 13 zeigt ein Beispiel für eine zertifizierende Behörde **500**. Die zertifizierende Behörde **500** stellt digitale Zertifikate **504** aus, die eine Umgebung für eine elektronische Rechteverwaltung bereitstellen. Die zertifizierende Behörde **500** kann die Erfüllung ihrer Aufgaben mit anderen Commerce Utility Systemen **90** koordinieren.

[0182] Die zertifizierende Behörde **500** stellt digitale Zertifikate **504** aus, die bestimmte Tatsachen zertifizieren. Das digitale Zertifikat **122** kann in gewisser Hinsicht mit einem Führerschein oder einem Abschlusszeugnis verglichen werden, da diese jeweils eine bestimmte Tatsache belegen. Beispielsweise können wir unseren Führerschein vorzeigen um zu beweisen, dass wir alt genug sind, um zu wählen, alkoholische Getränke zu kaufen oder uns einen Spielfilm mit Altersbeschränkung anzusehen.

[0183] Dieser Führerschein attestiert die Tatsache, dass wir einen bestimmten Namen sowie einen bestimmten Wohnsitz haben und dass wir über ein gewisses Wissen verfügen (von den staatlichen Gesetzen, denen die Kraftfahrzeuge unterliegen) und Fertigkeiten (die Fähigkeit, ein Kraftfahrzeug zu führen). Das digitale Zertifikat **504** ähnelt in dieser Hinsicht einem Führerschein, indem es die Identität des Lizenznehmers und relevante Tatsachen über den Lizenznehmer bestätigt, nur, dass es aus digitalen Daten besteht und nicht aus einer laminierten Karte.

[0184] In diesem Beispiel kann die zertifizierende Behörde **500** Anfragen des Verbrauchers und relevante Belege **502** empfangen sowie entsprechende digitale Zertifikate **504** ausstellen, die bestimmte Tatsachen zertifizieren. Die zertifizierende Behörde **500** kann überdies Belege, Credentials und ggf. auch Zertifikatdefinitionen von anderen Personen wie öffentlichen Behörden **506**, Berufsverbänden **508** und Universitäten **510** empfangen. So könnte die zertifizierende Behörde **500** beispielsweise Geburtsurkunden-Daten oder andere Identitäts-bezogenen Daten von einer öffentlichen Behörde **506** empfangen. Auf Grundlage dieser Identitäts-bezogenen Daten kann die zertifizierende Behörde **500** ein digitales Zertifikat **504** erstellen und ausstellen, das die Identität und das Alter einer Person attestiert. Die zertifizierende Behörde **500** könnte auch digitale Zertifikate **504** ausstellen, die auf der Grundlage verschiedener Belege **35** und Angaben von verschiedenen Personen einen Berufsstand, ein Beschäftigungsverhältnis, einen Wohnsitzstaat oder verschiedene andere Klassen und Kategorien belegen.

[0185] Die zertifizierende Behörde **500** kann Zertifikate für Organisationen und Maschinen als auch für Personen ausstellen. Die zertifizierende Behörde **500** könnte beispielsweise ein Zertifikat ausstellen, das die Tatsache attestiert, dass die Stanford University eine anerkannte Hochschuleinrichtung ist oder dass die ACME Transportation Company ordnungsgemäß eingetragen und geführt wird sowie befugt ist, Gefahrenstoffe zu befördern. Die zertifizierende Behörde **500** könnte beispielsweise auch ein Zertifikat **504** für einen Computer ausstellen, das die Tatsache attestiert, dass der Computer einer bestimmten Sicherheitsstufe entspricht oder befugt ist, Mitteilungen im Namen einer bestimmten Person oder Organisation abzuwickeln.

[0186] Die zertifizierende Behörde **500** kann mit der geschützten Verarbeitungsumgebung **154** und mit anderen Parteien kommunizieren, indem sie mit diesen elektronische Container **152** austauscht. Die geschützte Verarbeitungsumgebung **154** des elektronischen Geräts **100** kann die durch die zertifizierende Behörde **500** ausgestellten digitalen Zertifikate **504** benutzen, um Berechtigungen **188** zu verwalten oder auszuüben wie etwa jene, die durch das Rechte- und Berechtigungs-Clearinghaus **400** ausgestellt werden. Set-Top-Box **106** könnte beispielsweise Verbraucher unter 17 Jahren automatisch daran hindern, sich bestimmtes Sendungsmaterial anzusehen, oder sie könnte Schülern und Studenten für die Betrachtung von Bildungsmaterial einen Nachlass gewähren, wobei dies alles auf der Grundlage der durch die zertifi-

zierende Behörde **500** ausgestellten Zertifikate **504** geschieht.

Sichere Verzeichnis-Dienste

[0187] Fig. 14 zeigt ein Beispiel für sichere Verzeichnis-Dienste **600**. Sichere Verzeichnis-Dienste **600** funktionieren etwa wie ein computerisiertes Telefon oder ein Name Services Director. Verbraucher **95** können eine Anfrage **602** senden, in der die benötigten Informationen spezifiziert sind. Die sicheren Verzeichnis-Dienste **600** können die Informationen „nachschlagen" und die Antwort **604** dem Verbraucher **95** bereitstellen. Sie sicheren Verzeichnis-Dienste **600** können bei der Erfüllung dieser Aufgaben mit anderen Commerce Utility Systemen **90** zusammenarbeiten.

[0188] Angenommen, die Verbraucher **95** möchten beispielsweise bei Joe's Pizza elektronisch eine Pizza bestellen. Sie entscheiden, welche Pizza sie bestellen möchten (z. B. große Käsepizza mit Wurst und Zwiebeln). Sie kennen jedoch nicht die elektronische Adresse von Joe's Pizza's (die wie eine elektronische Telefonnummer sein kann). Die Verbraucher **95** können die Fernbedienung **108** benutzen, um ihre Suchanfrage einzugeben („Joe's Pizza, Lakeville, Connecticut"). Die geschützte Verarbeitungsumgebung **154** kann eine Anfrage **602** mit den Identifikationsdaten generieren und diese Anfrage an die sicheren Verzeichnis-Dienste **600** senden. Es kann die Anfrage in einem sicheren Container **152a** verschicken.

[0189] Wenn die sicheren Verzeichnis-Dienste **600** die Anfrage **602** erhalten, können sie auf eine Datenbank zugreifen, um die angeforderten Informationen zu lokalisieren. Möglicherweise hatten die Verzeichnis-Dienste **600** die elektronische Adresse von Joe schon zuvor direkt von Joe oder einer anderen Quelle bezogen. Die sicheren Verzeichnis-Dienste **600** können die angeforderten Informationen in einer Antwort **604** zurück an Gerät **100** senden. Die Antwort **604** kann auch in einem sicheren Container **152b** übertragen werden. Die Verbraucher **95** können diese Informationen benutzen, um auf elektronischem Wege ihre Bestellung an Joe's Pizza zu senden, die binnen weniger Sekunden nach ihrer Versendung durch die Verbraucher am Bestell-Terminal von Joe angezeigt wird. Joe kann dem Verbraucher **95** einige Minuten später eine ofenfrische, mit Käse, Wurst und Zwiebeln belegte Pizza liefern (mit dem Lieferwagen, nicht elektronisch, da eine echte Pizza um einiges besser schmeckt als eine elektronische).

[0190] Sichere Verzeichnis-Dienste **600** können beliebigen, mit dem Netzwerk **150** verbundenen Personen dabei helfen, beliebige andere Personen zu kontaktieren. Die sicheren Verzeichnis-Dienste **600** können beispielsweise dem Usage-Clearinghaus **300** mitteilen, wie es ein Finanz-Clearinghaus 200 im Netzwerk **150** finden kann. Jedes mit dem Netzwerk **150** verbundene elektronische Gerät **100** könnte auf sichere Verzeichnis-Dienste **150** zurückgreifen, um ein beliebiges anderes elektronisches Gerät zu kontaktieren.

[0191] Wie vorstehend erwähnt, kann die Versendung der Anfrage **602** an die sicheren Verzeichnis-Dienste **600** und die Rücksendung der Antwort **604** in sicheren Containern **152** von jenem Typ erfolgen, wie er in der Patentschrift von Ginter et al. beschrieben wird. Die Benutzung der sicheren Container **152** hilft dabei, Lauschangriffe auf den Datenaustausch zwischen den Verbrauchern **95** und den sicheren Verzeichnis-Diensten **600** zu verhindern. Dadurch wird der Verbraucher-Datenschutz sichergestellt. Die Verbraucher **95** machen sich möglicherweise wenig Sorgen, ob sie beim Bestellen einer Pizza belauscht werden, werden aber ein deutlich größeres Interesse daran haben, dass ihre elektronische Korrespondenz mit bestimmten anderen Personen geschützt wird (z. B. mit Ärzten, Banken, Anwälten oder anderen Personen, zu denen Sie eine Vertrauensbeziehung unterhalten). Sichere Container **152** können auch helfen sicherzustellen, dass über das Netzwerk **150** versandte Nachrichten authentisch sind und nicht verändert wurden. Dank der elektronischen Container **152** kann sich Joe's Pizza darauf verlassen, dass die soeben eingegangene Pizza-Bestellung tatsächlich von den Verbrauchern **95** stammt (und nicht von einer anderen Person) und nicht verändert wurde, und die Verbraucher können sich relativ sicher sein, dass niemand in ihrem Namen Joe eine gefälschte Pizza-Bestellung zuschickt. Die Benutzung der sicheren Container **152** und der geschützten Verarbeitungsumgebung **154** in der bevorzugten Ausführungsform trägt überdies dafür Sorge, dass die Verbraucher **95** anschließend nicht leugnen können, bei Joe's Pizza eine Bestellung aufgegeben zu haben, wenn sie dies getan haben.

Transaktionsbehörde **700**

[0192] Fig. 15 zeigt ein Beispiel für eine Transaktionsbehörde **700**. Die Transaktionsbehörde **700** stellt in diesem Beispiel Prozesssteuerung und -automatisierung bereit. Sie trägt dafür Sorge, dass Abläufe und Transaktionen erfolgreich ablaufen. Die Transaktionsbehörde **700** kann bei der Erfüllung und Ausführung ihrer Aufgaben mit anderen Commerce Utility Systemen **90** zusammenarbeiten.

[0193] Genauer überwacht die Transaktionsbehörde **700** in diesem Beispiel den Status einer elektronischen Transaktion und/oder eines elektronischen Vorgangs und führt sichere und zuverlässige Aufzeichnungen über Ereignisse, die bis dahin stattgefunden haben und solche, die bis zum Abschluss der gesamten Transaktion/des gesamten Vorgangs noch anstehen. Die Transaktionsbehörde **700** kann bei Be-

darf auch eine aktivere Rolle übernehmen, indem sie beispielsweise Anfragen für bestimmte Aktionen generiert. Die Transaktionsbehörde **700** kann in bestimmten Fällen der einzige Teilnehmer in einer komplexen Transaktion oder einen komplexen Vorgang sein, der sämtliche Schritte des Vorgangs „kennt". Transaktionsbehörde **700** kann auch auf der Grundlage von verschiedenen Teilnehmern des Vorgangs beigesteuerter elektronischer Steuermechanismen einen übergreifenden Vorgang elektronisch definieren.

[0194] Fig. 15 illustriert am Beispiel, wie Transaktionsbehörde **700** dazu verwendet werden kann, den Verbrauchern **95** die Möglichkeit zu geben, Handelsgüter wie einen Pullover zu bestellen. In diesem konkreten Beispiel für elektronisches Teleshopping (welches der Veranschaulichung dient und keinen Anspruch auf Vollständigkeit erhebt) können die Verbraucher **95** mit ihrer Fernbedienung **108** einen bestimmten Verkäufer auswählen sowie Schnitt und Farbe des Pullovers bestimmen, den sie zu einem bestimmten Preis bestellen möchten. In diesem Beispiel für Teleshopping kann die geschützte Verarbeitungsumgebung **154** von Gerät **100** eine elektronische Bestellung **702** generieren, die sie an die Auftragsannahme **704** eines Unternehmens sendet, das elektronische Bestellungen per Mail entgegennimmt. Die Bestellung **702** kann in einem sicheren Container **152a** verschickt werden.

[0195] In diesem Beispiel kann Transaktionsbehörde **700** das Unternehmen, das elektronische Bestellungen per Mail entgegennimmt, bei der Koordination von Aktivitäten unterstützen und dafür Sorge tragen, dass sämtliche Schritte, die für die Lieferung des Pullovers erforderlich sind, präzise und pünktlich abgearbeitet werden. Beispielsweise:

- Bei Eingang der elektronischen Bestellung **702** könnte die Auftragsannahme **704** eine elektronische Mitteilung **706** an die Transaktionsbehörde **700** schicken. Die Transaktionsbehörde **700** speichert die elektronische Mitteilung **706** und kann eine „Anfrage" ausgeben **708**.
- Die Transaktionsbehörde **700** hat ggf. die Anforderung **708** vor dem Eingang der Bestellung ausgegeben, sodass die Auftragsannahme **704** ihre Aufgaben bereits kennt, wenn eine Bestellung eingeht.
- Gemäß „Anforderung" **708** kann die Auftragsannahme **704** eine elektronische und/oder gedruckte (oder andere) Version der Bestellung **710** an die Fertigungsabteilung **712** ausgeben.
- Die Transaktionsbehörde **700** kann eine Fertigungsanforderung **714** an die Fertigungsabteilung ausgeben, damit diese den Pullover gemäß Kundenwunsch herstellt.
- Die Transaktionsbehörde **700** könnte auch eine Lieferanforderung **716** an den Lieferanten **718** ausgeben. Beispielsweise kann Transaktionsbehörde **700** beim Lieferanten **718** Ausgangsstoffe wie etwa Garnrollen **711** anfordern, damit der Hersteller **712** das für die Fertigung des Pullovers erforderliche Ausgangsmaterial hat.
- Der Lieferant **718** kann die Transaktionsbehörde **700** durch Ausgabe einer Mitteilung **720** unterrichten, wenn er die Ausgangsstoffe geliefert hat.
- Wenn die Fertigungsabteilung **712** den Pullover fertig gestellt hat, kann sie Transaktionsbehörde **700** durch Ausgabe einer Mitteilung **722** benachrichtigen.
- Bei Erhalt der Mitteilung **722** der Fertigungsabteilung **712** kann die Transaktionsbehörde **700** eine Versandanforderung **724** an Versandabteilung **726** ausgeben, beispielsweise indem sie die Versandabteilung auffordert, den fertig gestellten Pullover **728** in der Fertigungsabteilung abzuholen und an den Verbraucher zu liefern.

[0196] Die Transaktionsbehörde **700** kann ihre Aktivitäten mit anderen Commerce Utility Systemen **90** wie etwa einem Finanz-Clearinghaus **200** koordinieren, um die Zahlung zu veranlassen.

[0197] Dieses Beispiel dient selbstverständlich nur der Veranschaulichung. Die Transaktionsbehörde **700** kann für die verschiedensten Formen der Prozesssteuerung und -automatisierung verwendet werden wie beispielsweise die Abwicklung elektronischer Bestellungen und Verkäufe, den elektronischen Datenaustausch (Electronic Data Interchange, EDI), elektronische Vertragsverhandlungen und/oder -abschlosse, elektronische Zustellung von Dokumenten, Transaktionen innerhalb eines Unternehmens und zwischen Unternehmen und sichere elektronische Integration geschäftlicher Abläufe innerhalb von Unternehmen oder zwischen Unternehmen, um nur einige von vielen nutzbaren Anwendungen zu nennen.

VDE-Administrationsdienste **800**

[0198] Der VDE-Administrator **800** (siehe Fig. 1 der vorliegenden Anmeldung und Fig. 1A und die diesbezügliche Besprechung in der Patentschrift von Ginter et al.) kann in der bevorzugten Ausführungsform verschiedene Funktionen der elektronischen Unterhaltung und andere Funktionen beim sicheren, störungsfreien und effizienten Betrieb des Netzwerks **150**, der geschützten Verarbeitungsumgebungen **154** von Gerät **100** und des Distributed Commerce Utility **75** bereitstellen. Der VDE-Administrator **800** kann beispielsweise für die elektronische Sicherheit im Netzwerk **150** verwendete kryptographische Schlüssel verwalten, und überdies Dienste für die Pflege sicherer Daten durch Geräte **100**, die verschiedenen Commerce Utility Systeme **90** und andere elektronische Geräte bereitstellen. Wie in der Offenbarung des Patents von Ginter et al. ausführlich beschrieben, umfassen andere wichtige Funktionen

des VDE-Administrator **800** die Installation und Konfiguration geschützter Verarbeitungsumgebungen **154**, und die Unterstützung geschützter Verarbeitungsumgebungen bei der sicheren Führung hinterlegter Berechtigungen und/oder Benutzungsdaten. Der VDE-Administrator **800** kann mit anderen Commerce Utility Systemen **90** zusammenarbeiten.

Commerce Utility Systeme **90** können einander unterstützen

[0199] Commerce Utility Systeme **90** können nicht nur Verbraucher **95**, sondern auch andere Commerce Utility Systeme unterstützen. Dies wird den Fig. 16A-Fig. 16F gezeigt. Zum Beispiel:

- Finanz-Clearinghaus **200** kann dazu beitragen, dass andere Commerce Utility Systeme **90** für ihre Beiträge bezahlt werden (siehe Fig. 16A); und
- Usage-Clearinghaus **300** (siehe Fig. 16B) kann andere Commerce Utility Systeme **90** mit Informationen darüber beliefern, wie die durch diese bereitgestellte Unterstützung benutzt wird. Usage-Clearinghaus **300** kann beispielsweise die zertifizierende Behörde **500** darüber unterrichten, wie die Zertifikate der zertifizierenden Behörde verwendet werden (sehr nützlich für die zertifizierende Behörde bei der Beurteilung der Höhe der von ihr getragenen potentiellen Verantwortung oder bei der Erkennung gefälschter Zertifikate).
- Fig. 16C zeigt, dass ein Rechte- und Berechtigungs-Clearinghaus **400** andere Commerce Utility Systeme **90** wie beispielsweise ein Finanz-Clearinghaus **200**, ein Usage-Clearinghaus **300**, ein weiteres Rechte- und Berechtigungs-Clearinghaus **400**, eine zertifizierende Behörde **500**, sichere Verzeichnis-Dienste **600**, und eine Transaktionsbehörde **700** unterstützen kann.
- Die zertifizierende Behörde **500** kann digitale Zertifikate **504** ausstellen, die den Betrieb eines oder mehrerer anderer Commerce Utility Systeme **90** zertifizieren (siehe Fig. 16D) und damit andere Commerce Utility Systeme **90** wie beispielsweise ein Finanz-Clearinghaus **200**, a Usage-Clearinghaus **300**, ein Rechte- und Berechtigungs-Clearinghaus **400**, eine weitere zertifizierende Behörde **500**, sichere Verzeichnis-Dienste **600** und Transaktionsbehörde **700** unterstützen.
- Fig. 16E zeigt, dass sichere Verzeichnis-Dienste **600** andere Commerce Utility Systeme **90** wie beispielsweise Finanz-Clearinghaus **200**, Usage-Clearinghaus **300**, Rechte- und Berechtigungs-Clearinghaus **400**, zertifizierende Behörde **500**, andere sichere Verzeichnis-Dienste **600'** und Transaktionsbehörde **700** unterstützen können.
- Fig. 16F zeigt, dass eine Transaktionsbehörde **700** andere Commerce Utility Systeme **90** wie beispielsweise ein Finanz-Clearinghaus **200**, ein Usage-Clearinghaus **300**, ein Rechte- und Berechtigungs-Clearinghaus **400**, eine zertifizierende Behörde **500**, sichere Verzeichnis-Dienste **600**, und eine weitere Transaktionsbehörde **700** unterstützen kann.

"Ein Stück vom Kuchen"

[0200] Die hier beschriebenen Commerce Utility Systeme **90** stellen wertvolle und wichtige Dienste und Funktionen bereit. Die Betreiber solcher Dienste können und sollten für die durch sie bereit gestellten Dienste entschädigt werden. Finanz-Clearinghäuser können als Commerce Utility Systeme **200** dafür Soge tragen, dass sie und andere Anbieter von Unterstützungsdiensten diese Entschädigung ohne eine Beeinträchtigung anderer Teilnehmer der elektronischen Gemeinschaft und Wertkette erhalten.

[0201] Bei der Unterstützung oder Entschädigung von Teilnehmern der Wertkette kann Commerce Utility System **90** (auf Grundlage im Vorfeld bestätigter vertraglicher Vereinbarungen) für sich selbst einen Anteil bzw. Prozentsatz einbehalten, um sich für die bereitgestellten Clearingdienste zu entschädigen. Unterstützungsdienste können auf Grundlage eines kleinen Anteils an der Zahlung (i. e. einer „Mikro-Zahlung") entschädigt werden, die für jede elektronische Transaktion fällig wird (ein „Stück vom Kuchen"). Anbieter können einige oder alle dieser Gebühren an Teilnehmer ihrer Wertkette auf verschiedene Weise abführen.

[0202] Es können verschiedene Klassen von Teilnehmern der Wertkette zur Entschädigung der Commerce Utility Systeme **90** herangezogen werden, unter anderem:

- Verbraucher von Informationen (wie beispielsweise Personen, die sich den Informations-„Ausstoß" zunutze machen, der durch Aktivitäten des elektronische Handels, des elektronischen Transaktionsmanagements und der Rechteverwaltung entsteht);
- Rechteinhaber an Inhalten und andere elektronische Anbieter;
- Teilnehmer verschiedenster sicherer verteilter Transaktionen im elektronischen Handel;
- Ferner können verschiedene Anbieter von Unterstützungsleistungen auch auf verschiedene Unterstützungsleistungen anderer Anbieter angewiesen sein, sodass sich die Anbieter gegebenenfalls auch untereinander entschädigen müssen.

Beispielsweise:

- Ein Commerce Utility System **90** kann als Zwischeninstanz für den Kunden eines weiteren Commerce Utility Systems **90** fungieren;
- Ein Commerce Utility System **90** kann eine Aufforderung erhalten, den Betrieb eines weiteren Commerce Utility Systems **90** zu unterstützen; und/oder

• Commerce Utility Systeme **90** müssen möglicherweise bei der Abwicklung einer gemeinsamen Transaktion zusammenarbeiten.

[0203] Unterschiedliche Commerce Utility Systeme **90** können zusammenarbeiten, um eine gemeinsame Gebühr zu erheben, die sie dann untereinander aufteilen. In einem anderen Szenario kann jedes Commerce Utility System **90** unabhängig den Wert der von ihm erbrachten Dienste selbst in Rechnung stellen. Unterschiedliche Commerce Utility Systeme **90** können qualitativ und preislich miteinander konkurrieren, wie inzwischen auch Kreditkartenunternehmen um Anbieter und Verbraucher konkurrieren.

Beispiel für eine Architektur eines Distributed Commerce Utility Systems

[0204] Die Offenbarung des Patents von Ginter et al. beschreibt auf S. 180 ff. und zeigt in Fig. 10-Fig. 12 beispielsweise ein "Rechte-Betriebssystem", dass eine kompakte, sichere, ereignisgesteuerte, kompartimentierte, dienstebasierte, Komponenten-orientierte, verteilte, im Multiprocessing-Betrieb arbeitende Betriebssystemumgebung bereitstellt, die VDE-Sicherheitskontrollinformationen, Komponenten, und Protokolle in traditionelle Betriebssystemkonzepte integriert. Die bevorzugte, gemäß der vorliegenden Erfindungen bereitgestellte exemplarische Architektur eines Commerce Utility Systems **90** basiert auf dem von Ginter et al. beschriebenen Rechte-Betriebssystem und entwickelt dieses weiter.

[0205] Die bevorzugte exemplarische Architektur eines Commerce Utility Systems **90** stellt beispielsweise eine Auswahl an Dienstfunktionen bereit, die das Rechte-Betriebssystem als Anwendungen ausführen kann. Diese Dienstfunktionen definieren verschiedene nutzbare Aufgaben, die ein beliebiges und/oder sämtliche Commerce Utility Systeme **90** möglicherweise erfüllen müssen. Diese Dienstfunktionen sind verteilbar, skalierbar und umnutzbar. Sie können in verschiedenen Kombinationen und Subkombinationen kombiniert werden – je nach Geschäftsmodell, um beispielsweise die für eine beliebige konkrete Implementierung des Commerce Utility Systems **90** gewünschte Gesamtfunktionalität bereitzustellen.

[0206] Fig. 17A zeigt ein Beispiel für die Gesamtarchitektur eines Commerce Utility Systems **90**, Fig. 17B zeigt ein Beispiel für die Anwendungsarchitektur eines Commerce Utility Systems und Fig. 17C stellt eine Dienstfunktion ausführlich dar.

[0207] Im Beispiel von Fig. 17B enthält zunächst die Architektur der Anwendungssoftware für ein Commerce Utility System **90** einen Deskriptor **90A** des Commerce Utility Systems. Der Deskriptor **90A** des Commerce Utility Systems enthält Informationen über das Commerce Utility System **90**, die dazu verwendet werden können, ein derartiges ein System und seine Möglichkeiten zu identifizieren, sowie eine beliebige Anzahl Dienstfunktionen **90B(1)**, **90B(2)**, ... zu beschreiben, zu aggregieren und/oder sich mit ihnen zu verbinden. Der Deskriptor **90A** des Commerce Utility Systems und die Dienstfunktionen **90B** können beispielsweise unter Verwendung objektorientierter Programmiertechniken implementiert werden um sicherzustellen, dass dieser Deskriptor und diese Dienstfunktionen modular und umnutzbar sind, wodurch auch im Detail geklärt wird, wie beim Commerce Utility System **90** angeforderte Aktionen tatsächlich ausgeführt und/oder implementiert werden.

[0208] Der Deskriptor **90A** des Commerce Utility Systems (1) kann auch für die Koordination der Abläufe von Dienstfunktionen **90B** verantwortlich sein. In diesem Beispiel wird Deskriptor **90A** dazu verwendet, Anfragen und andere Systemaktionen an die entsprechenden Dienstfunktionen **90B** zu richten und durch Bereinigung von Differenzen in Schnittstellen, Datentypen etc., die zwischen den Dienstfunktionen **90B** vorkommen können, dafür Sorge zu tragen, dass Aktionen, die mehr als eine Dienstfunktion erfordern, koordiniert werden, was auch dazu beiträgt, den Verfahrens-Gesamtablauf unter den verschiedenen Dienstfunktionen **90B** zu lenken. Beispiele für solche Dienstfunktionen **90B** sind unter anderem:

- Audit,
- Führen von Aufzeichnungen,
- Beaufsichtigung von Prozessen,
- Statusüberwachung,
- vollständige Prozessdefinition,
- Prozesssteuerung,
- Schnittstelle(n) mit Settlement-Services,
- Kapitaltransfer,
- Währungsumwandlung,
- Steuerberechnung und Besteuerung,
- Einrichtung eines Kontos und Zuordnung von Kennungen,
- Zahlungsaggregation,
- Zahlungsdisaggregation,
- Budget-Vorbewilligung,
- Statusanzeige,
- Bestätigung,
- unvollständige Ereignisaufzeichnung,
- Erzeugung von Anforderungen,
- Berichtserzeugung,
- Ereigniskonsequenzen,
- Kontenausgleich,
- Identitätsauthentifikation,
- Schaffung einer elektronischen Währung,
- Verwaltung von Ereignisdatenbanken,
- Routing-Datenbank,
- Erzeugung von Anfragen,
- Duplikation,
- Propagierung,
- Verwaltung einer Benutzungsdatenbank,
- Erstellung und Verarbeitung von Rechnungen,

- Marktforschung,
- Verhandlung,
- Verwaltung von Regelsatz-Datenbanken,
- Erstellung von Regelsätzen,
- Prozesssteuerungslogik,
- Ereignisfluss-Erzeugung,
- Routing,
- Archivierung,
- Verwaltung von Rechte- und Berechtigungs-Datenbanken,
- Verwaltung von Template-Datenbanken,
- Sprachverarbeitung im Handelsmanagement,
- Sprachverarbeitung in der Rechteverwaltung,
- Verwaltung von Werbungsdatenbanken,
- automatische Klassenerzeugung,
- automatische Klassenzuordnung,
- Notar,
- Siegelgenerator,
- digitale Zeitstempel,
- Fingerprint/Wasserzeichen,
- Angebote und Gegenangebote,
- Objekt-Registry,
- Zuordnung von Objektbezeichnern,
- Registrierung von Urheberrechten,
- Registrierung von Regelsätzen,
- Registrierung von Templates,
- Erstellung von Zertifikaten,
- Führung von Sperrlisten,
- Director Database Management,
- Datenbankabfrage und Antwortverarbeitung,
- andere Dienstfunktionen.

[0209] Fig. 17C ist eine detailliertere Darstellung einer Dienstfunktion **90B**. In diesem Beispiel setzt sich Dienstfunktion **90B** aus Deskriptor **90C** der Dienstfunktion und beliebig vielen Komponenten **90D(1)**, **90D(2)**, ... von Dienstanwendungen zusammen. Deskriptor **90C** der Dienstfunktion füllt eine Rolle aus, die jener von Deskriptor **90A** des Commerce Utility Systems ähnelt mit der Ausnahme, dass sich seine Aktionen auf die Dienstfunktion **90B** und auf die Komponenten von Dienstanwendung **90D** beziehen. Der Deskriptor **90C** der Dienstfunktion und die Komponenten **90D** von Dienstanwendungen können beispielsweise auch unter Einsatz objektorientierter Programmiertechniken implementiert werden um sicherzustellen, dass diese Komponenten des Deskriptors und der Dienstfunktionen modular und umnutzbar sind, wodurch auch im Detail geklärt wird, wie bei Dienstfunktion **90B** angeforderte Aktionen tatsächlich ausgeführt und/oder implementiert werden. In diesem Beispiel implementieren die Komponenten **90D** der Dienstanwendung die meisten Möglichkeiten von Dienstfunktion **90B**, indem Schritte oder Unterfunktionen von Dienstfunktion **90B** ausgeführt werden.

[0210] Fig. 17A zeigt eine exemplarische Architektur eines übergreifenden Commerce Utility Systems **90**. Die in diesem Beispiel dargestellte Gesamtarchitektur ist ein objektorientiertes System, in dem das Commerce Utility-Gesamtsystem **90** ein Einzelobjekt ist, das sich wiederum aus umnutzbaren Objekten von Dienstfunktion **90B** zusammensetzt. Diese Objekte von Dienstfunktion **90B** setzen sich aus umnutzbaren Komponenten (Objekten) **90D** einer Dienstanwendung zusammen. Beliebige oder alle dieser Objekte können auf die durch Unterstützungsdienst-Ebene **90-4** eines Commerce Utility bereitgestellten Dienste zurückgreifen, wie weiter unten genauer beschrieben wird. Die Architektur **90** des Commerce Utility Systems der gezeigten bevorzugten Ausführungsform basiert auf dem Rechte-Betriebssystem **90-1**, wie es in der Patentschrift von Ginter et al. (siehe etwa Fig. 12 von Ginter et al.) genauer beschrieben wird. Ein Satz Dienstfunktionen **90B** enthält „Anwendungen", die durch das Rechte-Betriebssystem **90-1** ausgeführt werden. Es kann beliebig viele Dienstfunktionen **90B** geben.

[0211] Die objektorientierte Ausführung der Architektur von Commerce Utility Systeme **90** gemäß Fig. 17A hat mehrere wünschenswerte Eigenschaften. Ein Commerce Utility System **90** kann beispielsweise problemlos Dienstfunktionen **90B** hinzufügen, entfernen und/oder ersetzen, um seine Möglichkeiten zu verändern, erweitern und/oder verbessern. In ähnlicher Weise ermöglicht die Architektur ein Hinzufügen, Entfernen und/oder das Austauschen von Komponenten **90D** einer Dienstanwendung, um für den Fall einer Dienstfunktion eine ähnliche Flexibilität möglich zu machen. Überdies gestaltet die objektorientierte Ausführung die Umnutzung von Dienstfunktionen und/oder Komponenten einer Dienstanwendung in verschiedenen Commerce Utility Systemen **90** oder verschiedenen Dienstfunktionen **90B** (wie in Fig. 17A dargestellt) wesentlich einfacher und effizienter.

[0212] Die Anwendungsebene, bestehend aus Ebene **90-2** einer Dienstfunktion und Ebene **90-3** einer Dienstanwendungskomponente (umfassend Komponenten $\mathbf{90D_A}$) kann bei Bedarf durch Ebene **90-4** von Commerce Utility-Unterstützungsdiensten unterstützt werden. Ebene **90-4** der Commerce Utility-Unterstützungsdienste kann eine verbesserte Effizienz für eine große Anzahl Transaktionen bereitstellen. Beispiele für solche Commerce Utility-Unterstützungsdienste **90-4** sind etwa:

- Sitzungsmanagement,
- Fehlertoleranz,
- Speicherverwaltung,
- Lastausgleich,
- Datenbank-Bridging, und
- Commerce Utility-Unterstützungsdienste.

[0213] In diesem Beispiel sind die Dienstfunktionen **90B** Komponenten-basiert und können auf die Komponenten **90D** einer umnutzbaren und Komponenten-basierten Dienstanwendung zurückgreifen. Die

Komponenten **90D** einer Dienstanwendung führen typischerweise Schritte oder Unterfunktionen der Dienstfunktionen **90B** aus. Jede der Komponenten **90D** einer Dienstanwendung kann einen oder beide der folgenden Teile enthalten:
eine Komponente **90-B_a**, die nicht innerhalb der geschützten Verarbeitungsumgebung **154** ausgeführt werden muss; und
eine sichere Komponente **90-B_b**, die innerhalb der geschützten Verarbeitungsumgebung **154** ausgeführt werden muss.

[0214] In dieser exemplarischen Architektur können Komponenten **90D_a** und Komponenten **90D_b** einander entsprechen. Beispielsweise kann mindestens eine Komponente **90D_a** mindestens einer sicheren Komponente **90D_b** entsprechen. Möglich ist eine eineindeutige Entsprechung zwischen den Komponenten **90-D_a** und den Komponenten **90D_b** (wie in Fig. 17A durch gemeinsame geometrische Formen veranschaulicht). Sofern erforderlich und/oder gewünscht erlaubt diese Trennung von Funktionen in der bevorzugten Ausführungsform die Interaktion zwischen sicheren Abläufen innerhalb von PPE **154** und Komponenten **90D** einer Dienstanwendung. Durch Benutzung dieser Architektur ist es einfacher und effizienter, Dienstfunktionen zu schaffen, die sowohl das Implementieren von Eigenschaften einer Unterstützung auf Anwendungsebene als auch einer sicheren Verarbeitung erfordern.

[0215] Beispielsweise können einige durch Commerce Utility Systeme **90** ausgeführte Administrations- und/oder Unterstützungsfunktionen die Verwendung sowohl von Datenbankfunktionen auf Anwendungsebene als auch solcher Informationen umfassen, die durch eine geschützte Verarbeitungsumgebung („PPE", Protected Processing Environment) **154** in der bevorzugten Ausführungsform geschützt sind. Ein konkretes Beispiel hierfür wäre die Aufzeichnung von Zahlungen des Benutzers eines Finanz-Clearinghauses **200**. Wenn der Betreiber eines solchen Finanz-Clearinghauses **200** sich dafür entscheidet, Aufzeichnungen über Zahlungen in einer Datenbank auf Anwendungsebene abzulegen, gleichzeitig jedoch durch PPE **154** geschützte Informationen benötigt, um den aktuellen Kontostand eines Kunden präzise bestimmen zu können, so kann die Implementierung der Komponente **90D_A** einer Dienstanwendung, die die Informationen in der Datenbank auf Anwendungsebene mit durch PPE **154** geschützten und durch Komponente **90D_B** einer Dienstanwendung in ein Einzelobjekt verarbeiteten Informationen koordiniert, die Aufgabe der Verwendung dieser Informationen in der Umgebung einer bestimmten Dienstfunktion **90B** (z. B. die Entscheidung, einen Zusatzkredit zu gewähren) deutlich vereinfachen. Ferner kann diese exemplarische Komponente einer Dienstanwendung in anderen Dienstfunktionen **90B** umnutzbar sein.

[0216] In einem weiteren Beispiel könnte Komponente **90D_A** einer Dienstanwendung grundsätzlich auch als Objekt auf Anwendungsebene an der Schnittstelle zu einem entsprechenden Objekt von PPE **154 90D_B** fungieren. Wenn beispielsweise eine Notar-Dienstfunktion **90B** die Verwendung einer digitalen Signatur erfordert, so könnte die Komponente **90D_A** einer Dienstanwendung grundsätzlich eine Schnittstelle bereitstellen, die Daten zu und von einer Komponente **90D_B** einer entsprechenden Dienstanwendung transportiert, die im Wesentlichen sämtliche der für die Erstellung und Anwendung einer digitalen Signatur tatsächlich erforderlichen Aufgaben erledigt. Ferner könnte die Komponente **90D_A** der Anwendungsebene zusätzliche Funktionen der Unterbrechungsbehandlung, Protokollwandlung oder andere Funktionen bereitstellen, welche die Aufgabe haben, bestimmte Eigenschaften in einfacher Weise oder auf eine andere Weise als ursprünglich vorgesehen für eine Dienstfunktion **90B** zu integrieren.

[0217] Fig. 17D-1 zeigt ein Beispiel für eine Entsprechung zwischen Dienstfunktionen **90B** und allgemeinen Typen nutzbarer exemplarischer Commerce Utility Systeme **90**. Beispiele für Dienstfunktionen **90B** („Audit", „Führung von Aufzeichnungen", ...) sind horizontal dargestellt. Diese exemplarischen Dienstfunktionen **90B** können für die Implementierung exemplarischer Typen des Commerce Utility Systems **90** („Finanz-Clearinghaus", „Usage-Clearinghaus", ...) genutzt werden, die in die Zellen oben in der Abbildung vertikal eingetragen sind. Die Darstellung in Fig. 17D-1 erhebt keinen Anspruch auf Vollständigkeit – es sind auch weitere nutzbare Typen von Commerce Utility Systemen und sowie weitere Dienstfunktionen **90B** möglich. In diesem Sinne trägt die Architektur von Commerce Utility System **90** dafür Sorge, dass beide Typen und Dienstfunktionen **90B** in Abhängigkeit davon, wie sich die Geschäftsmodelle oder andere Faktoren wandeln, erweitert werden können.

[0218] Wenngleich bestimmte Geschäftserfordernisse und -modelle unabhängig von der konkreten Implementierung die Verwendung bestimmter Kombinationen und Zusammenstellungen wichtiger Dienstfunktionen tendenziell nahe legen können, ist doch die Architektur von Commerce Utility System **90** an sich flexibel und erlaubt bei der Implementierung die freie Mischung und Kombination einer Anzahl verschiedener Dienstfunktionen in Abhängigkeit von den jeweiligen Erfordernissen.

[0219] Beispielsweise ist es sinnvoll, ein Commerce Utility System **90** bereitzustellen, das als ein „Finanz-Clearinghaus **200**" fungiert und hierbei Zahlungsverarbeitung, Datenverkehr, Datenbankverwaltung und andere relevante Dienstfunktionen bereitstellt. Die Architektur eines Commerce Utility Systems kann ein solches "Finanz-Clearinghaus" bereit-

stellen und ist selbst auch in viel größerem Maße verallgemeinert und verallgemeinerbar. Eine bestimmte Implementierung eines Commerce Utility Systems **90** eines „Finanz-Clearinghauses" könnte beispielsweise auch „nichffinanzielle" Diensffunktionen mit finanziellen Diensffunktionen kombinieren. Die in einer bestimmten Implementierung eines Commerce Utility Systems **90** realisierten konkreten Funktionen oder Sätze von Funktionen hängen von den individuellen Bedürfnissen des Implementors ab, beispielsweise nach den Erfordernissen von Geschäftsmodell(en) oder -funktionen.

[0220] Fig. 17D-2 zeigt beispielsweise wie die übergreifende Funktionalität eines exemplarischen Commerce Utility Systems **200** vom Typ eines „Finanz-Clearinghauses" aus exemplarischen Dienstfunktionen **90B** zusammengesetzt sein kann. In diesem Beispiel sind die fett umrandeten Diensffunktionen **90B** Teil des Commerce Utility System Deskriptor **90a** gemäß Fig. 17B. Fig. 17D-2 zeigt ein exemplarisches Commerce Utility System **300** vom Typ eines Usage-Clearinghauses, das auf der Grundlage einer anderen Teilmenge fett umrandeter Diensffunktionen **90B** (gemäß Fig. 17D-1) zusammengesetzt ist. Beim Vergleich der Fig. 17D-2 und Fig. 17D-3 wird deutlich, dass manche Dienstfunktionen **90B** (beispielsweise „Audit", „Statusanzeige", „Verwaltung der Ereignisdatenbank" etc.) sowohl für Finanz- als auch für Usage-Clearing-Vorgänge umgenutzt werden können. Eine Commerce Utility System **90** vom Typ eines kombinierten Finanz- und Usage-Clearinghauses könnte den Verband der in Fig. 17D-2 fett umrandeten Dienstfunktionen **90B** und der in Fig. 17D-3 fett umrandeten Diensffunktionen **90B** benutzen. Mehr, weniger und/oder abgewandelte Funktionalität kann für ein bestimmtes Commerce Utility System **90** einfach dadurch bereitgestellt werden, dass mehr, weniger und/oder abgewandelte Dienstfunktionen **90B** bereitgestellt und abgerufen werden.

Verteilen des Commerce Utility Systems **90**

[0221] Die oben beschriebenen Komponenten **90-3** einer sicheren Anwendung können in der bevorzugten Ausführungsform reziproke Kontrollstrukturen und relevante Regeln und Verfahren gemäß **Fig.** 41A-41D und Fig. 48 der Patentanmeldung von Ginter et al. umfassen oder enthalten. Diese reziproken Kontrollstrukturen können dazu benutzt werden, verschiedene oder gleiche, im selben oder in verschiedenen Commerce Utility Systemen **90** oder anderen elektronischen Geräten **100** betriebene Regelsätze miteinander zu verbinden. Folglich kann jeder Akteur eine oder mehrere reziproke Beziehungen mit jedem anderen Akteur eingehen, wobei Commerce Utility System **90** an einigen Rollen einiger der unterschiedlichen Aktionen beteiligt ist.

[0222] Fig. 17E-1 bis Fig. 17E-4 zeigen verschiedene exemplarische Interaktionsmodelle, gemäß denen Commerce Utility System **90** teilweise auf Grundlage dieser reziproken Kontrollstrukturen mit einer laufenden Transaktion oder einem laufenden Vorgang interagieren kann:

- Fig. 17E-1 zeigt ein Modell für die Ereignisvermittlung, in dem ein Commerce Utility System **90** von einer sicheren Einheit (beispielsweise einer ersten geschützten Verarbeitungsumgebung) eine Ereignisanzeige **748** empfängt und Ereignis **758** generiert, das Aktivitäten einer weiteren (und/oder derselben) sicheren Einheit (beispielsweise einer zweiten und/oder der ersten geschützten Verarbeitungsumgebung) auslöst.
- Fig. 17E-2 zeigt ein anderes Interaktionsmodell für ein Commerce Utility System, in dem die erste sichere Einheit sowohl dem Commerce Utility System **90** als auch einer weiteren sicheren Einheit eine Ereignisanzeige **748** bereitstellt, um einen Schritt auszuführen, während die zweite Einheit auf eine Berechtigung von Commerce Utility System **90** wartet, bevor sie mit dem nächsten Schritt des Vorgangs fortfahren kann.
- Fig. 17E-3 zeigt ein Benachrichtigungsmodell, in dem Commerce Utility System **90** eher die Rolle eines passiven Betrachters einnimmt, der zum Zweck des sicheren Auditing Ereignisanzeigen **748** empfängt, hierüber hinaus jedoch mit dem laufenden Vorgang oder der laufenden Transaktion nicht direkt interagiert, sofern dies nicht erforderlich ist, um Ablaufunterbrechungen (beispielsweise einen Fehlerzustand) zu beheben.
- Fig. 17E-4 zeigt ein Vorautorisierungsmodell, in dem Commerce Utility System **90** an eine sichere Einheit als Reaktion auf den Empfang einer Ereignisanzeige **748** von dieser Einheit eine Benachrichtigung **748** ausstellen muss, bevor diese Einheit die Ereignisanzeige **748** an die nächste sichere Einheit übergeben kann, um den nächsten Schritt eines Gesamtvorgangs oder einer Gesamttransaktion ausführen zu können.

[0223] Die verschiedenen Interaktionsmodelle für Commerce Utility System **90** gemäß Fig. 17E-1 bis Fig. 17E-4 erheben keinen Anspruch auf Vollständigkeit bzw. schließen einander nicht aus; eine beliebige gegebene Transaktion bzw. ein beliebiger gegebener Vorgang kann auf der Grundlage von Geschäftsmodellen oder anderen Anforderungen umfassen einige oder alle von ihnen in verschiedenen Kombinationen.

[0224] Wie vorstehend erwähnt, stellen die vorliegenden Erfindungen Techniken für die Verteilung des Betriebs einer bestimmten Dienstfunktion **90-2** oder Komponente **90-3** einer Dienstanwendung in einem System **50** oder Netzwerk wie etwa auf elektronische Geräte eines individuellen Verbrauchers **95** bereit. Fig. 17F zeigt ein Beispiel für einen Regelsatz **188**, der dazu verwendet werden kann, eine rechnerferne geschützte Verarbeitungsumgebung (beispielsweise

ein verbraucherseitiges elektronisches Gerät) zu steuern, um einen „lokalen" Abschnitt eines Clearingvorgangs auszuführen. Ein Commerce Utility System **90** könnte diesen Regelsatz **188** an ein verbraucherseitiges elektronisches Gerät, an ein weiteres Commerce Utility System **90** oder ein anderes elektronisches Gerät (beispielsweise ein solches, das Teil einer Kommunikations-Infrastruktur ist) senden. Das Commerce Utility System **90** kann beispielsweise einen Teil seiner Clearingbefugnisse (implementiert beispielsweise in Form einer oder mehrerer Dienstfunktionen **90-2** mit jeweils einer oder mehreren Komponenten **90-3** einer Dienstanwendung) an einen Vorgang delegieren, der innerhalb der geschützten Verarbeitungsumgebung **154** eines benutzerseitigen elektronischen Geräts ausgeführt werden kann.

[0225] Das Beispiel von Fig. 17F ist ein Verfahren **850** (beispielsweise Messen, Fakturierung oder Budget), dessen AUDIT-Ereignis **852(1)** durch ein Audit-Verfahren **854** verarbeitet wird. Das exemplarische Messverfahren **850** könnte beispielsweise folgendes umfassen:

- ein BENUTZEN-Ereignis **852(2)** (beispielsweise Zähler „anklicken"),
- ein INITIALISIEREN-Ereignis **852(1)** (beispielsweise den Zähler einsatzbereit machen),
- ein ZURÜCKSETZEN-Ereignis **852(3)** (beispielsweise den Zähler nach einem Fehlerereignis auf einen bekannten gültigen Zustand zurücksetzen),
- ein AUDIT-Ereignis **852(4)** (beispielsweise Bereitstellung von während BENUTZEN-Ereignissen generierten Aufzeichnungen, sowie einer Kopie des aktuellen UDE-Werts und Veranlassung des Versands an den/die Auditor(en)),
- ein READ-USE-RECORD-Ereignis **852(5)** (beispielsweise eine Kopie der angeforderten Benutzungsaufzeichnung zurückgeben),
- ein LESEN-BENUTZEN-Ereignis **852(6)** (beispielsweise eine Kopie des aktuellen UDE zurückgeben),
- ein LESEN-MDE-Ereignis **852(7)** (das beispielsweise eine Kopie des angeforderten MDE zurückgibt), und
- verschiedene andere Ereignisse.

[0226] In diesem Beispiel kann das AUDIT-Ereignis **852(4)** mit einem Audit-Verfahren **854** verknüpft werden. Um in diesem Beispiel Zugriff auf die Daten zu bekommen, benötigt das Commerce Utility System **90** möglicherweise eine Berechtigung in Form von Zugriffs-Tags und/oder eines entsprechenden PERC-Regelsatzes, der genauere Nutzungsberechtigungen definiert, sowie semantisches Wissen vom Satzformat wie vom USE-Ereignis **852(2)** des Messverfahrens **850** verwendet. Das semantische Wissen könnte aus einem Out-of-Band-Agreement (beispielsweise einem Standard) oder aus einem Zugriff auf MDE (oder auf einen relevanten MDE-Abschnitt) von Messverfahren **850** bezogen werden, aus dem das Format der Benutzungsaufzeichnung ersichtlich wird.

[0227] Die Ereignisse von Audit-Verfahren **854** würden ein USE-Ereignis **856(2)** umfassen, das die vom Ereignis der rufenden Methode erwarteten Funktionen ausführt – in diesem Fall durch Zusammenstellung von Benutzungsaufzeichnungen und einer Kopie des aktuellen UDE sowie durch Versand dieser Daten. Angenommen, im Verfahren dieses Beispiels gibt es außerdem ein INITIALISIEREN-Ereignis **856(1)**. Das INITIALISIEREN-Ereignis **856(1)** würde unmittelbar nach seinem Aufruf intern versandt, und das (die) dazugehörige(n) Lademodul(e) würde(n) zum LESEN-MDE-Ereignis **852(7)** von Messverfahren **850** zurückrufen, um die Semantik der Use Records in Erfahrung zu bringen. Hiernach würde das USE-Ereignis **856(2)** aufgerufen und die mit der Verarbeitung dieses Ereignisses beschäftigten Lademodul(e) **858(2)** würden die betreffenden Ereignisse von Messverfahren **850** (beispielsweise mehrmalig READ USE RECORD, und einmalig READ UDE) aufrufen. An diesem Punkt sind die Erwartungswerte der rufenden Methode mit Ausnahme des administrativen Objekt-Packaging und der Übertragung erfüllt.

[0228] Durch mehr Verarbeitung durch das USE-Ereignis **856(2)** können mehr verteilte Clearingfunktionen implementiert werden. Während beispielsweise das Audit-Verfahren **854** die BENUTZEN-Aufzeichnungen vom Zähler einliest, kann sie Analysefunktionen implementieren (beispielsweise Typisierung der verwendeten Objekte und Reduzierung der über die Clearing-Kette transportierten Informationen auf eine einfachen Zählung, wie oft auf welche Inhaltstypen zugegriffen wurde). Aufzeichnungen von irrelevanten Inhaltstypen können verworfen werden. Die detaillierten Aufzeichnungen selbst können nach der Analyse verworfen werden. In einem weiteren Beispiel können die UDE-Werte (beispielsweise wie viele Klicks aufgezeichnet wurden) mit der Anzahl abgerufener Benutzungsaufzeichnungen verglichen werden, und im Fall einer Diskrepanz können sie gemeldet und/oder lokal beeinflusst werden (beispielsweise durch Deaktivierung des Gebrauchs von Objekten eines bestimmten Anbieters bis zur nächsten Interaktion). In einem weiteren Beispiel können Informationen über die Identität der Benutzer zur Wahrung des Datenschutzes aus den Aufzeichnungen entfernt werden. In einem weiteren Beispiel können einige Benutzungsaufzeichnungen lokal verarbeitet und analysiert (und hiernach verworfen) werden, während andere detaillierte Aufzeichnungen für die spätere Verarbeitung gespeichert werden.

[0229] Nachdem die verteilten Clearingfunktionen ausgeführt wurden, können die Informationen für den Transport in der Clearingkette in eines oder mehrere Administrationsobjekte an einen zentralisierten Ort

gepackt werden. Dies kann beispielsweise eine direkte Meldung an den (die) Anbieter und/oder eine Meldung an eine andere Clearingfunktion umfassen. Die verarbeiteten Aufzeichnungen können bei Erhalt, Verarbeitung, Übermittlung oder Erhalt einer Bestätigung durch die Empfänger (zur Löschung, Zusammenfassung, Archivierung etc. durch das Messverfahren) durch Audit-Verfahren **854** freigegeben werden.

[0230] In einem weiteren Beispiel unter Verwendung von Messverfahren **850** gemäß Fig. 17F könnte das AUDIT-Ereignis **854** intern durch die Messverfahren **850** ausgeführt werden. In diesem Beispiel würden die Benutzungsaufzeichnungen und UDE für die Übertragung zu dem (den) Auditor(en) durch die im Zusammenhang mit dem AUDIT-Ereignis **854(4)** von Messverfahren **850** verwendeten Lademodul(e) **853** in einem oder mehreren Administrationsobjekten gebündelt werden. Allerdings wäre es möglich, diese Objekte nicht zu übertragen, sondern vielmehr lokal zu verarbeiten. Hierfür könnte die Name Service Aufzeichnung, die durch das Rechte-Betriebssystem (s. Ginter et al. Fig. 12 und Fig. 13) verwendet wird, um den (die) Auditor(en) namentlich zu identifizieren, an die lokale geschützte Verarbeitungsumgebung (PPE) **154** zurückgesandt werden. In PPE **154** kann ein durch Commerce Utility System **90** gesteuerter Prozess (auf der Grundlage von Verfahren und/oder im Namen von Clearingfunktionen gelieferter Lademodule) erstellt werden, um die vorangehend beschriebenen lokalen Clearingfunktionen auszuführen, mit der Ausnahme, dass statt Anforderungen an Messverfahren-bezogene Ereignisse der Inhalt der Administrationsobjekt(e) verwendet wird. Dies weist eine stärkere Analogie zu jener Funktion auf, die in einer entfernten Clearingeinrichtung ausgeführt würde, und zwar dahingehend, dass die Vorgänge an Administrationsobjekten und ihren Inhalten ausgeführt werden, die Verarbeitung hingegen im lokalen verbraucherseitigen elektronischen Gerät, in einem vernetzten Gerät erfolgen kann.

[0231] Durch eine solche Verteilung von Unterstützungsdiensten stehen zusätzliche Möglichkeiten bereit, die bei einer zentralisierten Architektur möglicherweise fehlen oder nicht zur Verfügung stehen. Beispielsweise könnte ein Rechte- und Berechtigungs-Clearinghaus einen lokalen Server innerhalb einer Organisation dafür abstellen, dass dieser Anfragen mitverfolgt und Kopien zuvor von der Organisation angeforderter Berechtigungen im Cache ablegt. Ein solches lokales Rechte- und Berechtigungs-Clearinghaus könnte den Datenverkehr innerhalb des Netzwerks reduzieren und ein zweckmäßiges lokales Repository für Organisations-spezifische Berechtigungen (beispielsweise Site-Lizenzen für Computersoftware) bereitstellen. Der lokale Rechte- und Berechtigungsserver könnte von Rechteinhabern oder einer Rechte- und Berechtigungsstelle oder einer anderen Rechteverteilungs-Organisation die Vollmacht erhalten, auf Anfrage Genehmigungen zu erteilen.

[0232] In einem weiteren Beispiel können viele sichere, weitgehend automatisierte Administrations- und Unterstützungsdienste vollständig und/oder teilweise auf ein mindestens zeitweise angeschlossenes Gerät verteilt werden, ganz gleich, ob dieses Gerät ein Computer, eine Set-Top-Box, ein elektronischer Assistent (PDA-Computer), ein digitales Telefon, ein intelligenter Digitalfernseher oder ein anderes digitales Gerät ist. Solche Geräte können eine geschützte Verarbeitungsumgebung benutzen um sicherzustellen, dass der Unterstützungsdienst sicher, zuverlässig sowie geschützt gegen Manipulation und andere Einflüsse (beispielsweise wie in der Patentschrift von Ginter et al. beschrieben) betrieben wird.

[0233] In einem weiteren Beispiel umfasst ein mögliches Szenario der Verteilung von VDE-Inhalten Anbieter von Inhalten, welche das erste Packaging übernehmen, Verteiler, die Verteilungsfunktion übernehmen, Benutzer, die Benutzungsaufzeichnungen mitverfolgen sowie Clearinghäuser, die Benutzungs- und Finanzinformationen verarbeiten. Dem gegenüber steht ein zentralisiertes Verarbeitungsmodell, in welchen alle diese Funktionen einer einzigen zentralisierten Partei zufallen.

[0234] In einem weiteren Beispiel kann ein Effizienzwachstum durch die Verteilung von Clearinghausfunktionen über individuelle Benutzerrechner, über Server lokaler Netzwerke (LAN-Server) und/oder Gateway-Rechner von Unternehmen, welche die LAN-WAN-Umgebung eines Unternehmens mit der Außenwelt verbinden, sowie über kommerzielle Backbone-Server erreicht werden.

[0235] In einem weiteren Beispiel kann der Computer eines Unternehmens von einer zentralen zertifizierenden Behörde die Vollmacht erhalten, bestimmte Formen digitaler Zertifikate zu erteilen. Beispielsweise könnte das Unternehmen Mitglied einer bestimmten Handelsorganisation sein. Die zertifizierende Behörde der Handelsorganisation könnte ein digitales Zertifikat für das Unternehmen ausstellen, welches diese Tatsache attestiert, und an den Computer des Unternehmens die Zertifizierungsvollmacht delegieren, Zertifikate auszustellen, durch die attestiert wird, dass alle Beschäftigte des Unternehmens Mitglied der Handelsorganisation sind. In ähnlicher Weise können Eltern die Vollmacht erhalten, im Namen ihrer Kinder digitale Zertifikate auszustellen.

[0236] Die oben beschriebenen Techniken veranschaulichen, wie das Distributed Commerce Utility durch die Verwendung der Architektur von Commerce Utility System **90** über mehrere Commerce Utility Systeme verteilt werden kann. Ferner können die von

einem oder mehreren Commerce Utility System(en) **90** bereitgestellten Dienstfunktionen **90-2** in vollständige Verarbeitungsschritte oder gar Teilschritte zerlegt werden (beispielsweise Komponenten **90-2** einer Dienstanwendung), die je nach Wahl der Teilnehmer in einem bestimmten Szenario durch andere Commerce Utility Systeme **90** oder ein beliebiges anderes System (einschließlich Benutzersysteme) vollständig oder teilweise ausgeführt werden.

Exemplarische Typen von Commerce Utility Systemen

Finanz-Clearinghaus **200**

[0237] Fig. 18 zeigt ein Beispiel für ein Commerce Utility System **200** vom Typ eines Finanz-Clearinghauses. „Finanz-Clearinghäuser" unterstützen die automatisierte, effiziente finanzielle Erfüllung elektronischer Transaktionen. Finanz-Clearinghaus **200** kann beispielsweise zahlungsrelevante Informationen und Daten erfassen sowie auf effiziente Weise den Transfer von Geld und anderen Gegenleistungen veranlassen und damit sicherstellen, dass Werteanbieter bezahlt werden einschließlich der automatisierten, selektiven Disaggregation einer Zahlung in Teilzahlungen, die den entsprechenden Teilnehmern der Wertkette zugeführt werden. Finanz-Clearinghäuser **200** können geschützten Verarbeitungsumgebungen von Teilnehmern (beispielsweise Endanwendern) auch einen Kredit, Budgetlimits und/oder eine elektronische Währung bereitstellen, wobei das Finanz-Clearinghaus einige seiner Vorgänge für eine sichere lokale Ausführung solcher Vorgänge auf solche geschützten Verarbeitungsumgebungen **20** verteilen kann. Nachfolgend werden einige exemplarischen Unterstützungsfunktionen des Finanzclearings genannt, die mithilfe der vorliegenden Erfindungen bereitgestellt werden können:

- Sicheres, effizientes, pünktliches und korrektes Clearing von Finanz-Transaktionen.
- Bereitstellung eines sicheren Finanz-Clearings von Zahlungsmechanismen, die für Werteanbieter und Benutzer/Verbraucher vertrauenswürdig und zweckmäßig sind.
- Sicherstellung von Zahlungen an Rechteinhaber und andere Teilnehmer der Wertkette (beispielsweise Anbieter, die auf dem Weg von der Schaffung über den Vertrieb, Verkauf bis hin zur Lieferung die elektronische Gemeinschaft mit Werten beliefern), ohne dass diese mit einer großen Anzahl von Finanz-Schnittstellen, einer großen Kundenstreuung und/oder den verschiedensten, oft komplexen Finanzdienstleistungs-Standards und -Protokollen zurechtkommen müssen.
- Ausstattung der Verbraucher von Inhalten mit der Möglichkeit, für Informationsgüter und verwandte Dienste unter Verwendung einer Reihe verschiedener Zahlungsinstrumente über ein gemeinsame, vertrauenswürdige Schnittstelle zu zahlen.
- Ausstattung sämtlicher an einer Transaktion beteiligter Parteien mit der Möglichkeit zu verifizieren, dass ein bestimmter Austausch wie beiderseitig gewünscht stattgefunden hat, sowie eine Zurückweisung der Transaktion durch eine der Parteien auszuschließen.
- Kontenausgleich zum Zeitpunkt des Kaufs oder der Benutzungs-Berichterstattung (beispielsweise Zahlungsverkehr vom Konto eines Teilnehmers der Wertkette auf das Konto eines oder mehrerer Anbieter).
- Unterstützung von Clearingaktivitäten für viele kleine Transaktionen.
- Bereitstellung von Finanzclearingdiensten für alle Teilnehmer der Wertkette (beispielsweise Käufer, Händler und Verkäufer der verschiedensten digitalen Inhalte sowie Käufer, Händler, und Verkäufer physischer Waren und Benutzer anderer Dienste).
- Verknüpfung der Möglichkeiten des verteilten elektronischer Handels mit bestehenden Mitteln elektronischer, papiergebundener und/oder anderer Zahlung und/oder Clearingdiensten einschließlich, aber nicht beschränkt auf Kreditkartensysteme, Lastschriftkartensysteme von Banken, Smartcard-Systeme, elektronischen Datenaustausch, automatische Clearinghäuser, digitales Geld etc.
- Abwicklung und Abgleich durch eine oder mehrere Bank(en) und/oder andere Organisationen und/oder Verknüpfung direkt mit Einheiten, die Abwicklungsdienste rechtskräftig ausführen können.
- Erstellung und Zuweisung von Kennsätzen, Nummern, Namen oder anderen eindeutigen Kennungen durch eine oder mehrere Bank(en) und/oder andere Organisationen, an Ersteller digitaler Abläufe und/oder digitaler Informationen, Informationsverteilungen und/oder Modifikatoren und/oder Kunden- und/oder andere Benutzerkonten für Geldmittel, Gutschriften und Lastschriften.
- Benutzung sicherer Container in einem beliebigen Schritt, Teil oder Vorgang bei der Bereitstellung sicherer Finanz-Clearingdienste.
- Steuerung sicherer Abläufe des Finanzclearings, dies zumindest teilweise auf der Grundlage von Regeln und Steuermechanismen, die die Verteilung von Abläufen in jeder geschützten Verarbeitungsumgebung eines verteilten Finanz-Clearinghaus-Systems regeln, beispielsweise durch die benutzerseitigen geschützten Verarbeitungsumgebungen abgewickeltes Clearing, Webserver, zentralisierte Clearingeinrichtungen.
- Effiziente und sichere Umwandlung von einer Währung in eine andere.
- Ermöglichung einer Zahlungserfüllung bei Bereitstellung anderer Gegenleistung einschließlich Bearbeitungsgebühren, Produktgebühren und/oder beliebiger anderer Gebühren oder Kos-

ten mindestens teilweise auf Grundlage der Benutzung von Inhalten, Prozesssteuerung und/oder Rechteverwaltung.

• Unterstützung einer breiten Anwendung von Mikrogebühren und Mikrozahlungen zumindest teilweise auf der Grundlage von Inhalten, Prozesssteuerung und/oder anderen Benutzungs-Transaktionen, wobei diese Unterstützung die verteilte, sichere Akkumulation und/oder Verarbeitung von Aktivitäten mit Mikrotransaktions-Charakter und die periodische Übergabe von Informationen über solche Aktivitäten über ein Clearinghaus-Netzwerk zur weiteren Verarbeitung und/oder Akkumulation umfassen kann.

• Effiziente Messung und Verwaltung von Mikrozahlungsaktivitäten bei gleichzeitiger Minimierung der allgemeinen Transaktionskosten.

• Minimierung der Verarbeitungszeit von Mikrozahlungs-Transaktionen.

• Aggregation oder „Bündelung" von Transaktionen gegen lokalen Wertespeicher oder andere Zahlungsinstrumente (-verfahren).

• Verwendung von Regeln und Steuermechanismen für die Wertkette und einer Verarbeitungs- und Steuerungskette für eine effiziente Administration der Disaggregation (Splitting) von Zahlungen einschließlich der Übertragung oder des Transfers von Zahlungen an verschiedene Anbieter der Wertkette auf Grundlage derselben oder unterschiedlicher elektronischer Regelsätze, die Benutzungs- und/oder andere Berechtigungen steuern (beispielsweise sichere Steuerung von Zahlungskonsequenzen durch Parsen von Zahlungsbeträgen unter verschiedene Parteien der Wertkette gemäß den Regeln und Steuermechanismen, bevor bestimmte Zahlungsmethoden aktiviert werden.

• Reduzierung (beispielsweise Minimierung) der Anzahl der für die Unterstützung einer bestimmten Satzes von elektronischen Transaktionen erforderlichen elektronischen Nachrichten beispielsweise durch verteilte Transaktionsverarbeitung und/oder Akkumulation von Transaktionsaktivitäten.

• Unterstützung einer lokalen Aggregation (Bündelung oder Kombinierung) von Mehrfachzahlungen oder Mikrozahlungen am Standort des Wertketten-Teilnehmers.

• Ausstattung von Werteanbietern (beispielsweise Wertketten-Teilnehmern) mit der Möglichkeit, die Zahlungsfähigkeit eines anderen Wertketten-Teilnehmers effizient zu überprüfen, bevor er in Vorleistung Dienstleistungen oder Güter (physische und/oder elektronische) bereitstellt.

• Ausstattung von Werteanbietern mit der Möglichkeit, ein angemessenes Finanzierungsniveau für geschätzte Einkaufsniveaus am bevorzugten Zahlungsinstrument des Wertketten-Teilnehmers zu bewilligen, beispielsweise Bewilligung von Budgets für einen Kredit und/oder für eine Währung, der (die) für alle und/oder nur für bestimmte Transaktionsklassen (z. B. Inhalts- und/oder Prozesssteuerungstypen) eingesetzt werden kann einschließlich etwa Budgets für die Tätigung explizit spezifizierter Kategorien von Ausgaben wie beispielsweise nur Filme mit G-Einstufung und Filme mit PG-Einstufung (G rating: entspricht dem Deutschen „Freigegeben ohne Altersbeschränkung; R rating: empfiehlt eine vorherige Begutachtung oder Freigabe durch einen Elternteil).

• Verifizierung der Identität eines potentiellen Wertketten-Teilnehmers und Verknüpfung dieser Identität mit dem (den) Zahlungsinstrument(en) der Wahl des Wertketten-Teilnehmers.

• Bereitstellung einer periodischen Berichterstattung über Transaktions-Aktivitäten zum Zweck des Ausgleichs und der Erfassung durch Clearinghäuser. Abwicklung von Audits, Fakturierung, Zahlungserfüllung und/oder anderen Formen der Vergütung und/oder anderen Clearingaktivitäten.

• Bereitstellung einer ereignisgesteuerten Berichterstattung beispielsweise auf der Grundlage von Zeit, Ort, Erschöpfung lokaler Geldmittel und/oder Klasse der Auszahlungsaktivität wie etwa Zweck (für Geschäfts-, Unterhaltungs-, Reise-, Haushaltsausgaben), Familienmitglied oder eine andere Identität eines Individuums oder einer Gruppe, Kategorie eines Inhalts oder anderer erworbener Güter und/oder Dienstleistungen und/oder Kategorie eines beliebigen Typs einer Auszahlungsaktivität

• Empfang einer Vollmacht von einer sicheren Abwicklungs- und Steuerungskette in Form elektronischer Regelsätze.

• Erteilung einer Vollmacht und/oder Bereitstellung von Diensten an und/oder in Verbindung mit einem oder mehreren verteilten Finanz-Clearinghäuser(n), die einem oder mehreren dieser Clearinghäuser in einer bestimmten Kombination untergeordnet sind und/oder mit ihnen in einer Peer-to-Peer-Beziehung stehen.

• Verteilung von Finanzclearingfunktionen über ein Netzwerk oder ein anderes System (beispielsweise kann jeder Verbraucher- oder anderer Wertkettenteilnehmer-Knoten verteilte Finanzclearingdienste ausführen, wobei dieser Teilnehmerknoten Finanzclearing-Daten direkt an einen anderen oder mehrere andere Teilnehmer übermitteln kann) sowie gemäß den Regeln und Steuermechanismen und anderen VDE-Techniken wie beschrieben in der Patentschrift von Ginter et al.

• Erteilung einer Vollmacht und/oder Bereitstellung von Diensten für oder in Verbindung mit, einem oder mehreren untergeordneten Finanz-Clearinghäusern, deren Vorgänge von einem anderen Ort logisch und/oder physisch lokalisiert werden können wie etwa innerhalb eines Unternehmens oder einer Behörde und/oder innerhalb einer oder mehrerer Gerichtsbarkeit(en) und/oder im Dienst von Teilmengen des Gesamt-

geschäfts eines übergeordneten Finanz-Clearinghauses.

• Die Verteilung und/oder anderweitige Bewilligung von Finanzclearingfunktionen in einem System oder Netzwerk, beispielsweise wo jeder Verbraucher und/oder ein bestimmter anderer oder alle anderen Wertkettenteilnehmer-Knoten potentiell einen verteilten Usage-Clearingdienst unterstützen können, wodurch die eigenen sicheren Finanzclearing-Transaktionen und -Funktionen in der Umgebung des Clearinghaus-Gesamtnetzwerks auslöst werden, einschließlich Clearinghaus-Zusammenarbeit mit einem anderen Teilnehmer oder mehreren anderen Teilnehmern, interoperablen Knoten, wobei, wie auch in anderen Punkten dieser Aufzählung, alle Aktivitäten entsprechend auf VDE-Techniken zurückgreifen.

• Effiziente Berechnung, Einziehung, und Verteilung von Verkäufen und seitens mindestens einer Gerichtsbarkeit auferlegten „Mehrwertsteuern".

• Unterstützung eines Netzes aus Finanz-Clearinghäusern, in dem ein oder mehrere Klassen (Gruppen) von Clearinghäusern interoperable Peer-to-Peer Beziehungen unterhalten, und in dem unterschiedliche Gruppen mit unterschiedlichen Rechten der Zusammenarbeit mit Mitgliedern anderer Gruppen ausgestattet sein können, beispielsweise können Finanz-Clearinghäuser in geschützten Verarbeitungsumgebungen von Endanwendern über beschränkte Rechte der Zusammenarbeit mit „primären" Finanz-Clearinghäusern verfügen.

• Unterstützung eines Netzes aus geschützten Verarbeitungsumgebungen von Clearinghäusern, in dem solche geschützten Verarbeitungsumgebungen diskrete „Banken" oder geschützte Verarbeitungsumgebungen für die Abwicklung von Bankgeschäften enthalten, und wo solche geschützten Verarbeitungsumgebungen auf VDE-Möglichkeiten zurückgreifen können, um Banking-Funktionen sicher regeln und ausführen zu können wie etwa die sichere Hinterlegung (lokal und/oder rechnerfern) einer Notationswährung, das Recht, eine hinterlegte Währung an geschützte Verarbeitungsumgebungen von Endanwender-Clearinghäusern und/oder geschützte Verarbeitungsumgebungen anderer Clearinghäuser „zu verleihen", das Recht, elektronische Währungsobjekte herauszugeben, das Recht, Zahlungen von lokalen oder entfernten Währungsspeichern aus zu leisten, die Möglichkeit, zur Zahlung verpflichtenden Datenverkehr zu erhalten (beispielsweise elektronische Rechnungen), die Möglichkeit solche Zahlungen zu leisten, und die Möglichkeit, als eine Banking„Zweigstellen"-Komponente einer oder mehrerer virtueller Bank(en) (oder Banking-Netzwerk(e)) betrieben zu werden, wobei eine solche Bank viele der Rollen einer konventionellen Bank von heute ausfüllt.

• Unterstützung der Möglichkeit für Finanz-Clearinghäuser, eine elektronische Währung zu schaffen, die bedingt anonym ist, wobei eine solche Währung zur Erfüllung von Zahlungsverpflichtungen herangezogen werden kann und wobei eine solche Währung als authentisch gehandelt wird, ohne, dass sich die Empfängerpartei mit einer entfernten Banking-Behörde mit in Verbindung setzen muss, damit diese beurteilt, ob die Währung gültig oder für die Verwendung genehmigt ist.

• Unterstützung der Möglichkeit für verteilte geschützte Verarbeitungsumgebungen von Clearinghäusern, in tragbaren Geräten wie Smartcards (z. B. elektronischen Geldbörsen etc.) in Verbindung mit einer oder mehreren der oben beschriebenen Möglichkeiten betrieben zu werden, wobei mobile oder festnetzgebundene Kommunikationsmittel (oder andere Übermittlungsmechanismen) die Online-Übermittlung oder asynchrone Übermittlung von Informationen in Bezug auf eine aktuelle Transaktion oder eine Mehrfach-Transaktion wie Fakturierungs- oder andere Auditdaten über gewerbliche Tätigkeiten einschließlich der Identifizierung beispielsweise von Käufern, Verkäufern und/oder Vertreibern sowie Autorisierungsinformationen, Budgetinformationen, Informationen zur Kreditbereitstellung, Währungsbereitstellung und/oder Auszahlung etc. mit Bezug zu einer solchen Aktivität unterstützen.

• Unterstützung der Bereitstellung von Nachlässen, Zuschüssen und/oder Gutscheinen für Teilnehmer der Wertkette, beispielsweise an Verbraucher im Gegenzug für Benutzungsdaten oder feiner granulierte Benutzungsdaten (beispielsweise zur Verbesserung von Datenschutzaspekten in bestimmten Umgebungen).

• Kann hierarchisch, nach dem Peer-to-Peer-Prinzip oder in einer kombinierten Form organisiert sein, wobei die Verantwortung für das Finanz-Clearing für verschiedene Handelsmodelle und/oder Aktivitäten und/oder Wertketten auf verschiedene Weise verteilt sein kann, wobei eine bestimmte oder mehrere Parteien beispielsweise in einem Fall oder mehreren Fällen hierarchisch anderen Parteien übergeordnet, in einem anderen Fall oder mehreren anderen Fällen jedoch hierarchisch ein Peer oder untergeordnet sein kann (können).

• Die Beziehung zwischen Teilnehmern ist programmierbar und kann dergestalt eingerichtet (und nachträglich verändert) werden, dass für bestimmte gewerbliche Tätigkeiten, Wertketten oder Modelle eine oder mehrere gewünschte Finanzclearing-Konfiguration(en) entstehen.

• Verteilung von Zahlungen auf mehrere Parteien, wie etwa Steuern auf eine oder mehrere Regierungen (beispielsweise Stadtregierung, Bundesstaatsregierung und Landesregierung).

[0238] Fig. 18 zeigt ein Beispiel für ein funktionsori-

entiertes Schaubild für Finanz-Clearinghaus **200**. In diesem Beispiel ist Finanz-Clearinghaus **200** in hohem Maße automatisiert und wird in einer vertrauenswürdigen, sicheren Sphäre betrieben, um eine geschützte Verarbeitungsumgebung bereitzustellen. Es stellt effizient Finanz-Clearingdienste für alle möglichen Ketten im elektronischen Handel bereit. Es kann auch als Gateway zwischen der Sphäre der in hohem Maße sicheren virtuellen Verteilungsumgebung (virtual distribution environment, VDE) und anderen Sphären dienen und damit für die bestehende Infrastruktur eine Protokollunterstützung bereitstellen. Die Gateway-Funktionen können die hochflexiblen und verteilten geschützten VDE-Verarbeitungsumgebungen mit der Möglichkeit ausstatten, die unflexiblen und zentralisierten, dafür jedoch allerorts vorhandenen und vertrauenswürdigen bestehenden Dienste der Finanz-Infrastruktur nutzbar zu machen.

[0239] Die Kernfunktionen von Finanz-Clearinghaus **200** bestehen in der Zahlungsverarbeitung **208**, Zahlungsaggregation **212**, Zahlungsdisaggregation **214** sowie in der Verwaltung von Mikrozahlungen **216**, da durch diese Funktionen Geld von Kunden und anderen Teilnehmern der Wertkette eingezogen wird, und Geld an Anbieter von Dienstleistungen oder Produkten in der Wertkette wie etwa Händlern gezahlt wird.

[0240] Konkreter kann Finanz-Clearinghaus **200** in diesem Beispiel die folgenden Funktionen ausführen:

- Zahlungsverarbeitung **208**,
- Kreditchecks **210**,
- Zahlungsaggregation **212**,
- Zahlungsdisaggregation **214**,
- Abwicklung von Mikrozahlungen **216**,
- ereignisgesteuerte Berichterstattung **218**,
- Ausgleich **220**,
- Wartung/Pflege von Datenbanken **222**
- Replikation **224** und
- Propagierung **226**.

[0241] Finanz-Clearinghaus **200** kann Zahlungsdaten **202**, Kundendaten **230**, Anbieterdaten **232** sowie aggregierte Berichte und Rechnungen **234** von der Außenwelt empfangen. Es kann Abbuchungsaufträge **236**, Kreditaufträge **238**, Abschlüsse und Berichte **204**, **240**, Freigabesignale **242** sowie Kreditschecks und -Bewilligungen **244** erstellen.

[0242] Die Datenbankverwaltung **222** und die ereignisgesteuerte Berichterstattung **218** kann dazu verwendet werden, Teilnehmer der Wertkette sicher mit präzisen Finanzberichten zu versorgen. Die Ausgleichfunktion **220**, welche sowohl in der Berichterstattung als auch im Finanzmanagement verwendet wird, stattet das Finanz-Clearinghaus **200** mit der Möglichkeit aus, sein Finanzmanagement zuverlässigerer zu gestalten. Die Replikationsfunktion **224** und Propagierungsfunktion **226** werden durch Finanz-Clearinghaus **200** verwendet, um die verteilte Verarbeitung mit anderen Finanz-Clearinghäusern **200** und/oder anderen sicheren oder unsicheren geschützten Verarbeitungsumgebungen zu erleichtern, wodurch das Finanz-Clearinghaus in die Lage versetzt wird, Status- und Updateinformationen mit anderen Commerce Utility Systemen oder anderen Teilnehmern sicher gemeinsam zu nutzen.

[0243] Im gezeigten Beispiel stellen die Zahlungsdaten **202** (welche in einem oder mehreren sicheren Container(n) **152** eintreffen können) die Primäreingabe für Zahlungsverarbeitungsblock **208** dar. Zahlungsdaten **202** können erforderlichenfalls auch einige oder alle der an ein Usage-Clearinghaus **300** gesandten Benutzungsdaten umfassen, oder sie können unterschiedliche Typen von Benutzungsdaten umfassen, die für die Durchführung von Finanz-Audits und die Nachverfolgung von Transaktionen relevanter sind. Diese Zahlungsdaten **202** können in Realzeit oder zeitverzögert (beispielsweise periodisch oder auf andere Weise ereignisgesteuert) eintreffen.

[0244] Finanz-Clearinghaus **200** benutzt Anbieterdaten **232** und Kundendaten **230**, um Geldüberweisungen zwischen Kunden und Anbieter zu tätigen. Finanz-Clearinghaus **200** orientiert sich bei der Gesamtverarbeitung **208** der Zahlungen sowie bei der Zahlungsaggregation **212** und Zahlungsdisaggregation **214** an den aggregierten Berichten und Rechnungen **234**. Finanz-Clearinghaus **200** kann beispielsweise Abbuchungs- und Kreditaufträge **236**, **238** an dritte Finanzparteien wie Banken, Kreditkartenunternehmen etc. ausstellen, um Verbraucherkonten zu belasten und in den Konten der Anbieter die entsprechenden Gutschriften vorzunehmen. Finanz-Clearinghaus **200** kann für ein sicheres Auditing und/oder zu Informationszwecken Abschlüsse **204** und Berichte **240** ausstellen. Finanz-Clearinghaus **200** kann nach durchgeführten Kreditchecks **210** Kreditbewilligungen **244** ausstellen, womit der Kredit dem entsprechenden Teilnehmer der Wertkette gewährt wird. Eine solche Authentifikation **244** kann eine Eingabe-Ausgabe-Funktion enthalten, sofern sie nicht vollständig lokal ausgeführt wird (d. h., eine Bewilligungsanfrage trifft ein, und Clearinghaus **200** ist die Quelle der Kredit- und/oder Kreditlimitinformationen).

[0245] Finanz-Clearinghaus **200** kann unter gegebenen Umständen Freigabesignale **242** ausgeben, damit elektronische Geräte **100** die Hinterlegung von Finanzdaten einstellen und/oder noch nicht „quittierte" Finanzinformationen aufzubewahren können, nachdem diese durch Finanz-Clearinghaus **200** übertragen, analysiert und/oder verarbeitet wurden. In einem Beispiel kann das benutzerseitige Gerät **100** innerhalb der Grenzen des Geschäftsmodells die Finanzinformationen auch noch nach ihrer „Freigabe" speichern, aus ihnen einen Kurzbericht generieren etc. Selbstverständlich kann dies mit einer Kopie der

Daten auch schon zuvor geschehen sein (beispielsweise wenn vorher ein Zugriff auf die Daten genehmigt wurde). Angenommen beispielsweise die lokale Kopie von Finanz-Benutzungsdaten enthält vertrauliche Informationen über das Geschäftsmodell. Die Betrachtung einer Eigenschaft könnte $ 1,00 kosten, und dieser Dollar kann auf verschiedene Parteien aufgeteilt werden. In der Regel nimmt der Benutzer nur wahr, was unter dem Strich steht und nicht die Teilsummen, aus denen sich dieser Betrag zusammensetzt, obwohl lokal für jeden an der Transaktion Beteiligten eine Aufzeichnung existieren kann.

[0246] Fig. 19 zeigt ein Schaubild für eine exemplarische Architektur von Finanz-Clearinghaus **200**. Finanz-Clearinghaus **200** enthält in diesem Beispiel einen sicheren Kommunikationshandler **246**, einen Transaktionsverarbeiter **248**, ein Datenbankverwaltungsprogramm **250**, eine Weiche **252**, und einen oder mehrere Schnittstellenblöcke **244**. Diese exemplarische Architektur eines Finanz-Clearinghauses kann beispielsweise auf der Architektur des Betriebssystems gemäß Fig. 12 und Fig. 13 der Patentschrift von Ginter et al. basieren (der universelle externe Dienste-Manager **172** in diesem Beispiel könnte beispielsweise Schnittstellen **254** mit Abwicklungsdiensten unterstützen). Mithilfe des sicheren Kommunikationshandlers **246** kann Finanz-Clearinghaus **200** sicher mit anderen elektronischen Geräten **100(1)** ... **100(N)** kommunizieren. Ein solcher Datenverkehr kann in sicheren digitalen Containern **152** erfolgen. Bei den meisten Commerce Utility Systemen **90** (einschließlich Finanz-Clearinghaus **200**) ist es wünschenswert, den Empfang von Container **152** sowohl in Echtzeit als auch asynchron zu unterstützen. Ferner kann Finanz-Clearinghaus **90** auch ein Protokoll für Echtzeitverbindungen unterstützen, das auch ohne Container **152** auskommt und für einfache Transaktionen wie eine Kreditkartenzahlung ohne Erfordernis einer Disaggregation eingesetzt wird. Vorteil einer Echtzeitverbindung sind Ergebnisse in Echtzeit. Dies kann in solchen Fällen von Vorteil sein, wo Benutzer mehr Geld oder einen Kredit benötigen, weil ihre Mittel erschöpft sind (statt einfach einen Bericht zu erstellen oder eine periodische Wiederauffüllung eines Budgets zu erhalten, das noch nicht erschöpft ist), aber auch, wo ein Anbieter (beispielsweise von Inhalten oder Budgets) darauf besteht, dass zunächst eine Transaktion verrechnet wird, bevor eine Fortsetzung der Transaktion genehmigt werden kann, gleich welche Aktivität diese auslöste.

[0247] Eine Verbindung für eine Transaktion in Echtzeit erfordert nicht immer sichere Container **152**, aber auch in diesem Szenario bietet die Verwendung von Containern **152** Vorteile. Container **152** ermöglichen beispielsweise die Verknüpfung der Inhalte mit Regeln und Steuermechanismen, womit den Benutzern die Möglichkeit gegeben ist zu bestimmen, wie die Inhalte verwendet werden können. Ferner ermöglicht die Verwendung von Container **152** den wirksamen Einsatz bereits bestehender Möglichkeiten in der geschützten Verarbeitungsumgebung. Die Benutzung einer Technologie wie E-Mail, um Container **152** zuzustellen (beispielsweise als Anhänge an SMTP-Mail-Nachrichten oder als Anhänge an ein beliebiges anderes E-Mail-Protokoll, das Anhänge unterstützt), ermöglicht die asynchrone Verarbeitung von Inhalten und stattet Commerce Utility Systeme **90** somit mit der Möglichkeit aus, Spitzen bei den Verarbeitungslasten wegzunehmen. Ein Kostenfaktor beim Betrieb eines kommerziellen Clearinghauses sind die Abschreibungskosten der Ausrüstung. Die quantitative Ausstattung hängt im Wesentlichen von den Anforderungen während Spitzenlastzeiten ab. Es sind erhebliche Lastschwankungen zu erwarten (beispielsweise Freitag Abend um 20:00 Uhr im Vergleich zu Dienstag Morgen um 3:00 Uhr). Durch Nivellierung dieser Funktionen sind erhebliche Einsparungen bei der Ausrüstung und den damit verbundenen Kosten (Strom, Personal, Wartung etc.) möglich.

[0248] Transaktionsverarbeiter **248** kann empfangene Daten verarbeiten und analysieren, und das Datenbankverwaltungsprogramm **250** kann empfangene Daten in einer Datenbank zur späteren Analyse und/oder zur Analyse der History speichern (um Kreditlimits zu erhöhen, Zahlungs-Historys etc. zu analysieren). Ferner kann Datenbankverwaltungsprogramm **250** auch Daten über bestehende Kreditlimits, Adressen für den Datenverkehr (physische und/oder elektronische) und andere Kontodaten speichern. Die Patentschrift von Ginter et al. beispielsweise bespricht Budgetbelastungen. Das Datenbankverwaltungsprogramm **250** kann auch dazu verwendet werden, Informationen zu speichern, die nötig sind, um Belastungen zu verfolgen. Es können auch Sätze von Sicherheitsinformationen dazu verwendet werden, mit den geschützten Verarbeitungsumgebungen und/oder mit solchen Benutzern zu kommunizieren, die von den geschützten Verarbeitungsumgebungen und den Abwicklungsdiensten Gebrauch machen. Aufzeichnungen zum Datenverkehr mit den Abwicklungsdiensten können dort ebenfalls gespeichert werden. Die Datenbank **250** kann auch mit verschiedenen Einrichtungen für die Berichterstattung mit Bezug zu ihren Inhalten ausgestattet werden.

[0249] Transaktionsverarbeiter **248** und Datenbankverwaltungsprogramm **250** erfüllen zusammen die meisten der in Fig. 18 dargestellten Funktionen. Weiche **252** wird verwendet, um Daten zu und von den Schnittstellenblöcken **244** zu routen. Die Schnittstellenblöcke **244** werden für die Kommunikation mit dritten Abwicklungsdiensten wie Kreditkartenunternehmen, automatischen Clearinghaus-Systemen (Automatic Clearing House, ACH) für den Bankabrechnungsverkehr, Debitkartenkontos etc. benutzt. Optional können die internen, durch eine Federal Reserve

Bank **256** bereitgestellten Abwicklungsdienste anstelle von oder zusätzlich zu den dargestellten Abwicklungsdiensten Dritter verwendet werden, um einen Rechnungsabschluss gemäß den maßgeblichen Banking-Vereinbarungen und gesetzlichen Anforderungen bereitzustellen. Die von Finanz-Clearinghaus **200** verwendeten Zahlungsmechanismen können symmetrisch (z. B. VISA anweisen, das Konto von Verbraucher A zu belasten und dem Konto von Händler Y etwas gutzuschreiben) oder asymmetrisch (z. B. VISA anweisen, das Konto von Verbraucher A zu belasten und den Betrag an das Finanz-Clearinghaus zu übermitteln, damit dieses unter Verwendung eines anderen Zahlungsmechanismus den Betrag dem Konto von Händler Y gutschreibt) sein, sofern nach Maßgabe der anwendbaren Finanz- und Banking-Bestimmungen zulässig.

Beispiele für Finanzclearing-Vorgänge

[0250] Fig. 20 zeigt einen exemplarischen Finanz-Clearinghaus-Vorgang. In diesem Beispiel beliefert Anbieter **164** einen Verbraucher **95** mit Gütern, Dienstleistungen oder Inhalten. Beispielsweise kann Anbieter **164** ein oder mehrere digitale Eigenschaften **1029** und hiermit verbundene Steuermechanismen **404** in einem elektronischen sicheren Container **152** bereitstellen. Eine sichere geschützte Verarbeitungsumgebung **154** am Standort des Verbrauchers **95** verfolgt Zahlungs-, Benutzungs- und andere Informationen und kann eine Prüfkette **228** bereitstellen, die diese Informationen spezifiziert. Prüfkette **228** kann in einem oder mehreren sicheren Containern **152b** vom Standort des Verbrauchers **95** an das Finanz-Clearinghaus **200** übermittelt werden. Prüfkette **220** könnte beispielsweise die Identifikation des Bericht-erstattenden elektronischen Geräts **100**, den Zahlbetrag, die Identifikation des Anbieters, die vom Verbraucher gewünschte Zahlungsmethode, Name oder andere Identifikation des Benutzers des elektronischen Geräts und die Type(n) der beteiligten Transaktion(en) umfassen. Der Zeitpunkt und/oder die Häufigkeit der Berichterstattung könnte sich nach einer Anzahl verschiedener Ereignisse richten wie beispielsweise Tageszeit, Woche, Monat, Jahr oder anderes Zeitintervall; das Eintreffen eines hiermit verbundenen oder nicht verbundenen Ereignisses (z. B. es ist vorab eine Zustimmung zu einem Kauf erforderlich, eine bestimmte Anzahl Einkäufe hat stattgefunden, eine lokale elektronische Geldbörse ist erschöpft, es ist aus einem anderen Grund eine Berichterstattung erforderlich etc.), oder eine Kombination aus diesen.

[0251] Finanz-Clearinghaus **200** analysiert die Prüfkette **228** (Audit Trail) und generiert einen oder mehrere Kurzberichte **240**. Finanz-Clearinghaus **200** kann Anbieter **164** den Kurzbericht **240** durch elektronische Übermittlung in einem sicheren Container **152c** bereitstellen. Finanz-Clearinghaus **200** kann seine Vorgänge auch mit jenen eines Finanzmittlers **258** und eines oder mehrerer Finanzabwickler **260** koordinieren, um eine Bank oder ein anderes Konto von Verbraucher **95** zu belasten und eine entsprechende Gutschrift bei einer Bank oder einem anderen Konto des Anbieters **164** auszulösen.

[0252] Beispielsweise kann das Finanz-Clearinghaus **200** die Audit-Daten empfangen, die Transaktionen disaggregieren (in einzelne Wertketten-Beträge für Ersteller, Händler, und andere sowie für den Fiskus und andere öffentlichen Einheiten) und hiernach jenen Betrag ermitteln, der ihm jeweils von den Begünstigten der Transaktion geschuldet ist. Hiernach können, sofern gewünscht oder erforderlich, die Transaktionen (wegen des Umfangs der Transaktionen, per Transaktionsgebühren oder wegen anderer Effizienz- und/oder Kosten-bezogener Überlegungen) zu Gesamtbeträgen für jede der Parteien zusammengefasst und (zusammen mit den betreffenden Kontoinformationen) dem für Kreditkarten-Transaktionen verantwortlichen Finanzmittler **258** vorgelegt werden. Der Finanzmittler **258** (der auch Gebühren einziehen oder einen Prozentsatz einbehalten kann) kann anschließend die Transaktionen beim Finanzabwickler **260** dergestalt auslösen, dass die Begünstigten jeweils die entsprechenden Beträge erhalten. Alternativ kann das Finanz-Clearinghaus **200**, sofern es die Möglichkeit und die Vollmachten besitzt, die erforderlich sind, um Kreditkarten-Transaktionen direkt an Kreditkartenunternehmen zu übergeben, die Transaktionen direkt beim Finanzabwickler **260** (beispielsweise Visa) auslösen.

[0253] Finanzabwickler **260** kann Anbieter **164** (und/oder Verbraucher **95**) einen Abschluss **204** zusenden, in dem die stattgefundenen Soll- und Haben-Buchungen im Einzelnen aufgeführt werden. Bei Bedarf kann er Abschluss **204** in einem sicheren Container (nicht dargestellt) bereitstellen. Finanz-Clearinghaus **200** kann einen Teil oder Prozentsatz der eingezogenen Geldmittel erhalten, um für die von ihm bereitgestellten Finanzclearingdienste entschädigt zu werden.

[0254] Fig. 20A-Fig. 20F zeigen eine exemplarische Finanz-Clearing-Aktivität unter Verwendung einer lokalen elektronischen Geldbörse **262**, die am verbraucherseitigen elektronischen Gerät **100** unterhalten wird. In diesem Beispiel kann das Finanz-Clearinghaus **200** den Verbraucher **100** zunächst mit elektronischem Geld in Form bargeldloser Mittel durch Übermittlung der bargeldlosen Mittel in einem oder mehreren sicheren Containern **152** versorgen. Finanz-Clearinghaus **200** kann die Bank des Verbrauchers **206a** oder ein anderes Konto automatisch belasten, um diese Geldmittel zu erhalten, und es kann dies auf Verlangen des Verbrauchers tun (siehe Fig. 20A).

[0255] Das verbraucherseitige elektronische Gerät **100** kann nach Erhalt der elektronischen Geldmittel diese in einer elektronischen Geldbörse **262** aufbewahren, die es in seiner geschützten Verarbeitungsumgebung **154** (beispielsweise als ein „MDE" wie in Ginter et al. beschrieben) (siehe Fig. 20B) aufbewahrt. Das verbraucherseitige elektronische Gerät **100** kann dieses lokal gespeicherte elektronische Geld einsetzen, um vom Verbraucher konsumierte Waren und Dienste zu bezahlen. So kann beispielsweise ein Herausgeber **68** ein Werk **166** wie ein Buch, einen Film, ein Fernsehprogramm oder ähnliches für das verbraucherseitige elektronische Gerät bereitstellen, indem er dieses Werk in einem oder mehreren sicheren Container(n) **152b** übermittelt. Der Verbraucher kann sein elektronisches Gerät **100** bedienen, um den Container zu öffnen und Zugriff auf das Werk **166** zu bekommen, wonach er vom Werk gemäß den für dieses Werk spezifizierten elektronischen Steuermechanismen (siehe Fig. 20C) Gebrauch machen kann.

[0256] Angenommen, der Rechteinhaber fordert für die Benutzung des Werks **166** eine Zahlung, so kann das elektronische Gerät **100** des Verbrauchers die elektronische Geldbörse **262** automatisch um den geforderten Zahlbetrag (in diesem Fall $ 5) (Fig. 20C) betasten. Zusätzlich kann das elektronische Gerät **100** automatisch eine Benutzungsaufzeichnung **264** generieren, das dieses Benutzungsereignis registriert. Auf Grundlage eines Zeitereignisses und/oder eines anderen Ereignisses kann das verbraucherseitige elektronische Gerät **100** an das Finanz-Clearinghaus **200** in Form eines elektronischen Containers **152c** (siehe Fig. 20D) automatisch eine Prüfkette **264** versenden, die ein Paket Audit-Aufzeichnungen enthalten kann, welche zum Zeitpunkt des Auditing übermittelt werden, oder einen Satz hierzu gehöriger, in der sicheren Datenbank hinterlegter Aufzeichnungen (oder, um den Datenschutz des Verbrauchers zu gewährleisten, eine Zusammenfassung hiervon).

[0257] Finanz-Clearinghaus **200** kann nach Erhalt der Benutzungsaufzeichnung **262** und seiner erfolgreichen Abspeicherung in der eigenen Datenbank **250** mittels eines elektronischen Containers **152d** ein Freigabesignal **242** (siehe Fig. 20D) versenden. Dieses Freigabesignal **242** kann das verbraucherseitige elektronische Gerät **100** in die Lage versetzen, die bis zu diesem Zeitpunkt hinterlegte Benutzungsaufzeichnung **264** (siehe Fig. 20D) zu löschen.

[0258] Der Verbraucher kann dasselbe oder ein anderes Werk **166** ein weiteres Mal benutzen, um die Generierung einer weiteren Benutzungsaufzeichnung **264** auszulösen und die elektronische Geldbörse **262** mit einer weiteren Benutzungsgebühr zu belasten (wobei in diesem Fall die Mittel der Geldbörse erschöpft werden) (siehe Fig. 20E). Bei Erschöpfung der elektronischen Geldbörse **262** kann das verbraucherseitige elektronische Gerät **100** wieder Finanz-Clearinghaus **200** kontaktieren, um bei ihm zusätzliche Geldmittel anzufordern (siehe Anforderung **228**), und um eine Benutzungsaufzeichnung **264** bereitzustellen (beide Informationen werden in diesem Beispiel in demselben elektronischen Container **152e** übermittelt) (siehe Fig. 20F).

[0259] Finanz-Clearinghaus **200** kann (nach Belastung der Bank oder eines anderen Kontos des Verbrauchers) mit der Übermittlung zusätzlicher elektronischer Geldmittel antworten, sowie ein weiteres Freigabesignal bereitstellen, durch welches das verbraucherseitige elektronische Gerät **100** in die Lage versetzt wird, die Benutzungsaufzeichnung **264** zu löschen (siehe Fig. 20F). Das eingezogene Geld kann (nach Vornahme entsprechender Abzüge, um die Commerce Utility Systeme **90** zu entschädigen) an die Rechteinhaber ausgezahlt werden.

Zahlunasdisaggregation

[0260] Fig. 21 zeigt ein Beispiel für eine Finanzclearing-Aktivität unter Beteiligung einer Wertketten-„Disaggregation". Finanz-Clearinghaus **200** unterstützt in diesem Beispiel effizient, zuverlässig und sicher die Zahlungsdisaggregation innerhalb einer Wertkette. Fig. 21 zeigt einen Inhaltsersteller wie etwa einen Autor, der ein Werk **166** an einen Herausgeber **168** liefert. Der Herausgeber veröffentlicht das Werk (beispielsweise in einem elektronischen Buch **166**) und beliefert damit den Verbraucher **95**. In diesem Beispiel bezahlt der Verbraucher **95** $ 20 für sein Buchexemplar **166'**. Die Zahlung des Verbrauchers wird etwa auf Grundlage einer vertraglichen Absprache „disaggregiert" bzw. zwischen Autor **164** und Herausgeber **168** aufgeteilt. In diesem Beispiel erhält der Herausgeber vier der durch den Verbraucher bezahlten 20 Dollar, und der Autor erhält den Rest.

[0261] Mit Hilfe der Disaggregation kann Finanz-Clearinghaus **200** eine vom Verbraucher geleistete Zahlung automatisch auf beliebig viele verschiedene Teilnehmer der Wertkette aufteilen. Dies ist äußerst nützlich, wenn es darum geht, dass sämtliche Parteien, die an der Bereitstellung eines Produkts bzw. einer Dienstleistung beteiligt sind, zuverlässig und effizient für ihren jeweiligen Beitrag entschädigt werden.

[0262] Fig. 22 zeigt, wie Finanz-Clearinghaus **200** die Wertketten-Disaggregation gemäß Fig. 21 unterstützen kann. Im elektronischen Beispiel von Fig. 22 kann Kunde **95** seine Zahlung elektronisch an Finanz-Clearinghaus **200** leisten. Diese Zahlung kann in Form einer in einem sicheren elektronischen Container **152a** verpackten elektronischen Währung bereitgestellt werden oder in anderer Form (z. B. ausgewiesene Benutzungsdaten zusammen mit einer be-

reits bestehenden Vollmacht für Finanz-Clearinghaus **200**, das Bankkonto von Kunde **95** zu belasten).

[0263] Finanz-Clearinghaus **200** kann die entsprechenden Anteile der Kundenzahlung in Übereinstimmung mit der Vereinbarung zwischen dem Autor und dem Herausgeber auf Autor **164** und Herausgeber **168** aufteilen. Wie erfährt das Finanz-Clearinghaus **200**, wem die Teilbeträge der disaggregierten Zahlung zustehen? Im Beispiel dieser Fig. 22 kann das Werk **166** vom Autor **164** an den Herausgeber **168** und vom Herausgeber **168** an Kunde **95** in elektronischer Form in einem oder mehreren sicheren elektronischen Container(n) **152** übermittelt werden. Einer oder verschiedene Container können einen oder mehrere elektronische Regelsätze **188** enthalten, wobei diese Regelsätze den Umgang mit dem Werk **166** oder anderen Eigenschaften regeln. Die Regelsätze **188** können unter anderem den zu zahlenden Betrag festlegen, den der Kunde **95** für die Benutzung von Werk **166** schuldig wird.

[0264] Die Steuermechanismen **188** können auch festlegen und steuern, wie die Kundenzahlung unter den anderen Teilnehmern der Wertkette disaggregiert wird. So kann Autorin **164** mittels der von der Autorin bereitgestellten Steuermechanismen **188b** etwa bestimmen, dass ihr für jedes Exemplar des durch den Endverbraucher **95** erworbenen Werks **166** $ 16 zustehen. Dank der in Übereinstimmung mit der virtuellen Verteilungsumgebung bereitgestellten sicheren Kette der Verarbeitung und Steuerung (siehe die Offenbarung des Patents von Ginter et al.) kann Autor **164** (in dem durch die kommerziellen Prioritäten des Autors geforderten und dem bei der Leistungsfähigkeit des Gesamtsystems möglichen Grad) sich darauf verlassen, dass Herausgeber **168**, Kunde **95** und ein beliebiger anderer Verbraucher oder potentieller Benutzer der Eigenschaft **166** von Steuerung **188b** kontrolliert wird. Der Herausgeber **168** kann zu den von Autor **164** spezifizierten Steuermechanismen seine eigenen hinzufügen, wobei die Steuermechanismen des Herausgebers **188c** (beispielsweise) einen Aufpreis von $ 4 vorsehen, den er für die Benutzung seines Markennamens, seiner Vertriebs- und Marketing-Dienstleistungen einfordert.

[0265] Fig. 22A zeigt an einem detaillierten Beispiel, wie Zahlungsdisaggregation unter Verwendung der Regelsätze **188** wie in der Offenbarung des Patents von Ginter et al. beschrieben innerhalb der geschützten Verarbeitungsumgebung **154** des Kunden ausgeführt werden kann. Ginter et al. zeigt in Fig. 48 und dem dazugehörigen Text auf, wie ein Regelsatz einen übergreifenden Mess-, Fakturierungs- und Finanzplanungs-Vorgang in der geschützten Verarbeitungsumgebung **154** eines Benutzers implementieren und regeln kann. Fig. 22A illustriert die Zahlungsdisaggregation auf der Grundlage eines oder mehrerer, einer geschützten Verarbeitungsumgebung **154** eines Verbrauchers bereitgestellter Regelsätze **188**. Jeder der Verarbeitungsblöcke gemäß Fig. 22A kann die Reaktion auf eine Benutzeranforderung (auf das Ereignis einer Benutzeranforderung), Inhalte zu öffnen und auf Inhalte zuzugreifen sein.

[0266] In diesem konkreten Beispiel dient Messverfahren **275** dazu, ein Ereignis an Fakturierungsverfahren **277** immer dann zu übergeben, wenn der Verbraucher einen bestimmten Inhalt das erste Mal benutzt (Messereignis **275** könnte bei Bedarf auch oder alternativ das Ereignis jedes Mal übergeben, wenn der Verbraucher den Inhalt benutzt, um eine „Pay-per-View"-Funktionalität bereitzustellen).

[0267] Die Fakturierungsverfahren **277** umfassen in diesem Beispiel zwei verschiedene Fakturierungsverfahren **277a** und **277b**. Die Verfahren **277a** und **277b** können voneinander unabhängig übergeben werden – beispielsweise könnte der Autor **164** Fakturierungs-Subverfahren **277a** übergeben und der Herausgeber **168** könnte Fakturierungs-Subverfahren **277b** übergeben. Fakturierungsverfahren **277a** schreibt Informationen in eine Fakturierungslisten-Datenstruktur, in der spezifiziert wird, wie viel dem Autor **164** auszuzahlen ist (in diesem Beispiel $ 16). Fakturierungsverfahren **277b** schreibt Informationen in dieselbe oder eine andere Fakturierungslisten-Datenstruktur und spezifiziert, wie viel dem Herausgeber auszuzahlen ist ($ 4). Fakturierungsverfahren **277a** und **277b** können jeweils das offene, von Messverfahren **275** übergebene Ereignis empfangen, und sie können jeweils Fakturierungs-Aufzeichnungen in dieselbe (oder eine andere) Fakturierungslisten-Datenstruktur schreiben.

[0268] In diesem Beispiel kann ein Budgetverfahren **279** unabhängig von den Fakturierungsverfahren **277a** und **277b** übergeben werden. Budgetverfahren **279** kann Aufzeichnungen in eine Budgetlisten-Datenstruktur **281** schreiben, in der (unter anderem) die genaue Aufteilung bei der Zahlungsdisaggregation spezifiziert wird (d.h. die $ 16/$ 4-Aufteilung zwischen Autor und Herausgeber) gemäß den Fakturierungsverfahren **277a** und **277b**. Die Budgetlisten-Datenstruktur **281** (die unabhängig von den durch Fakturierungsverfahren **277a** und **277b** geführten Datenstrukturen geführt wird und daher von Autor **164** und/oder Herausgeber **168** nicht beeinflusst werden kann) könnte an ein Finanz-Clearinghaus **200** versandt werden. Das Finanz-Clearinghaus **200** würde die Finanzclearing-Aktionen Zahlung und Sollbuchung wie oben beschrieben ausführen, infolgedessen das Konto des Verbrauchers mit $ 20 belastet wird, das Konto des Autors eine Gutschrift von $ 16 erhält und das Konto des Herausgebers eine Gutschrift von $ 4 erhält (wodurch die Zahlung des Benutzers in Höhe von $ 20 zwischen Autor **164** und Herausgeber **168** disaggregiert wird). Zwischenzeitlich könnte die Fakturierungslisten-Datenstruktur an

ein von Autor **164** und/oder Herausgeber **168** vorgegebenes Usage-Clearinghaus **300** versandt werden. Usage-Clearinghaus **300** könnte die Fakturierungslisten-Datenstruktur analysieren und Autor **164** und/oder Herausgeber **168** wissen lassen, welche Zahlungen sie von Finanz-Clearinghaus **200** erwarten können.

[0269] Somit können elektronische Regelsätze **188** in diesem Beispiel unter anderem die folgenden Dinge vorgeben oder definieren: (I) in einem bestimmten digitalen Objekt verfügbare Rechte, (II) die Kosten der Ausübung solcher Rechte und (III) wie Zahlungen für die Ausübung dieser Rechte auf die Rechteinhaber aufgeteilt (disaggregiert) werden. Diese Möglichkeit, die Zahlungsdisaggregation im Voraus zu definieren (bevor Zahlungsmethoden und -vereinbarungen des Kunden aktiviert werden), stellt ein hohes Maß an Effizienz und Flexibilität bereit, da hierdurch die Zahlungsmethode des Verbrauchers beispielsweise dazu verwendet werden kann, um Teile der Zahlung des Verbrauchers automatisch solchen Personen zuzuführen, die entschädigt werden müssen. Da ein und dasselbe elektronische Gerät **100** dazu benutzt wird, die Rechte auszuüben und Zahlungen verschiedenen Teilnehmern der Wertkette zuzuleiten, wird ein Abschnitt des übergreifenden Finanzclearing-Ablaufs effektiv über eine große Anzahl paralleler Rechenressourcen verteilt. Wegen des hohen Maßes an Vertrauenswürdigkeit, das durch das in der Patentschrift von Ginter et al. offenbarte System bereitgestellt werden kann, können die Rechteinhaber solche Regelsätze **188** beispielsweise in den Handelsstrom mit entsprechender Gewissheit ausgeben, dass ihre Zahlungsvereinbarungen erfüllt werden. Finanz-Clearinghaus **200** kann dafür Sorge tragen, dass solche disaggregierten Zahlungen die erforderlichen Empfänger effizient und schnell erreichen.

[0270] Eine geschützte Verarbeitungsumgebung **154** am Standort von Kunde **95** setzt die erweiterten Steuermechanismen **188c** sicher durch, indem sie eine vollständige Zahlung und/oder eine Zahlungsermächtigung vom Kunden **95** als Bedingung dafür fordert, dass der Kunde einen Zugriff auf Werk **166** erhält. Die Steuermechanismen **188c** können auch vorgeben, welches Finanz-Clearinghaus **200** für die Zahlungsverarbeitung heranzuziehen ist und welche Zahlungsmethoden akzeptabel sind und dabei den Kunden **95** gleichzeitig hinsichtlich der Wahl der gewünschten Zahlungsmethode mit Flexibilität ausstatten. Die geschützte Verarbeitungsumgebung **154c** des Kunden kann hiernach für die Disaggregation gemäß den Steuermechanismen **188a** an Finanz-Clearinghaus **200** automatisch eine entsprechende Zahlung oder Zahlungsermächtigung **190a** versenden, wobei es sich um dieselben Steuermechanismen (oder eine Teilmenge dieser Steuermechanismen in Bezug auf die Zahlungsdisaggregation) handeln kann, die der Autor und/oder der Herausgeber vorgegeben hat.

[0271] Da die geschützte Verarbeitungsumgebung **154c** des Kunden Steuermechanismen **188a** generiert, die den durch den Herausgeber und Autor vorgegebenen Steuermechanismen **188c** und **188b** unterliegen (siehe Fig. 22), kann die Erfüllung der Zahlungswünsche des Autors und des Herausgebers bei Berücksichtigung der zwischen den beiden Parteien vereinbarten Zahlungsteilung diesen Zahlungs-Steuermechanismen **188a** anvertraut werden. Die geschützte Verarbeitungsumgebung des Kunden **154c** kann in einem oder mehreren sicheren elektronischen Container(n) **152a** die Kundenzahlung oder Zahlungsermächtigung **152a** und diese Zahlungs-Steuermechanismen **188a** an Finanz-Clearinghaus **200** senden.

[0272] Finanz-Clearinghaus **200** verarbeitet die Zahlung oder Zahlungsermächtigung **152a** gemäß den Steuermechanismen **188a**, indem es in Übereinstimmung mit der zwischen dem Autor und dem Herausgeber getroffenen Vereinbarung über die Zahlungsaufteilung Zahlung **152b** an den Herausgeber tätigt und Zahlung **152c** an den Autor tätigt. So könnte Finanz-Clearinghaus **200** beispielsweise $ 4 elektronisches Geld an den Herausgeber und $ 16 elektronisches Geld an den Autor versenden; oder es könnte der Bank oder anderen Konten des Autors und Herausgebers diese Beträge gutschreiben. Da dieser gesamte Vorgang in einer sicheren, vertrauenswürdigen virtuellen Verteilungsumgebung stattfindet, kann jeder der Teilnehmer der Wertkette darauf vertrauen, dass er die von i im geforderte Zahlung tatsächlich erhält, und der Vorgang automatisch und elektronisch auf sehr effiziente Weise ausgeführt werden kann, die einer großen Bandbreite an verschiedenen Geschäftsmodellen und Ad-hoc-Beziehungen flexibel Rechnung trägt.

[0273] Fig. 23 zeigt ein weiteres, etwas komplexeres Beispiel für Zahlungsdisaggregation, das die Wertkette um einen Verteiler oder Aggregator **170** von Inhalten erweitert. In diesem Beispiel müssen die $ 20 von Verbraucher **95** nun möglicherweise nicht in zwei, sondern in drei Teilsummen aufgeteilt werden, wobei Autor **164** nach wie vor $ 16 erhält, der Herausgeber nur $ 3 erhält und der Verteiler/Aggregator von Inhalten **170** für seine Leistungen $ 1 erhält. Fig. 24 zeigt, dass dieselbe Grundlösung gemäß Fig. 22 verwendet werden kann, um die Zahlung und andere Interessen dieses neuen Wertkette-Teilnehmers zu realisieren.

[0274] Fig. 25 zeigt ein weiteres Beispiel für eine Zahlungsdisaggregation. Fig. 25 zeigt, wie Disaggregation dazu verwendet werden kann, Commerce Utility Systeme **90** für ihre Rolle bei der Unterhaltung und Verwaltung der Wertkette zu entschädigen. Wie oben beschrieben, stellt das Distributed Commerce

Utility **75** sehr wichtige Dienste wie Finanz-Clearing, Benutzungs-Auditing, Permissioning, Zertifizierung etc. bereit. Ganze Geschäftszweige oder Branchen können auf einer effizienten und zuverlässigen Bereitstellung dieser Art von Administrations- und Unterstützungsdiensten gegründet sein. Commerce Utility Systeme müssen für ihre eigenen Investitionen und Leistungen entschädigt werden. Eine Möglichkeit ihrer Entschädigung besteht darin, dass sie von jeder Transaktion einen kleinen Teil erhalten, „ein Stück vom Kuchen". Dieselben Mechanismen der Zahlungsdisaggregation wie die oben beschriebenen können auch dazu verwendet werden, solche Mikrozahlungen an Commerce Utility Systeme **90** zu unterstützen.

[0275] Fig. 23 zeigt ein Beispiel, in dem die Commerce Utility Systeme **90** 3% (z. B. $ 0,60 im dargestellten Beispiel) des Wertes jeder Transaktion erhalten. Da die oben besprochenen elektronischen Regelsätze **188** dazu verwendet werden, solche Mikrozahlungs-Möglichkeiten zu implementieren, kann jedes gewünschtes Geschäftsumfeld oder -ziel flexibel und effizient realisiert werden.

[0276] Fig. 26 zeigt, dass Zahlungsdisaggregation dazu verwendet werden kann, eine einzige Verbraucher-Zahlung bei Vorhandensein verschiedener Ziele und unter Verwendung verschiedener Zahlungsmechanismen (beispielsweise Kreditkarten, Bankkonten, elektronisches Geld etc.) in eine beliebige Anzahl unterschiedlicher Beträge zu disaggregieren bzw. aufzusplitten (und für den internationalen Handel gar Beträge in verschiedenen Währungen auszuweisen).

[0277] Fig. 27 und Fig. 28 zeigt noch weitere Beispiele für Zahlungsdisaggregation, um ein weiteres Mal zu illustrieren, mit welcher Flexibilität das Distributed Commerce Utility **75** mit diesen und anderen Anordnungen umgehen kann. Im Beispiel von Fig. 27 wird gezeigt, wie die Kundenzahlung auf den Autor **164**, den Herausgeber **168**, den Aggregator **170**, einen Repackager **174** und zwei zusätzliche Autoren **164a** und **164b** aufgesplittet wird, die zusätzliche Werke liefern, welche Teil der dem Kunden bereitgestellten elektronischen Eigenschaft sind. Das Beispiel von Fig. 27 gilt besonders beispielsweise für Szenarien, in denen der Repackager **174** verschiedenen Quellen Inhalte zu verwandten Themen entnimmt und diese zu Produkten unterschiedlicher Quellen zusammenstellt, etwa zu multimedialen Kombinationen, Paketen zu aktuellen Themen oder Newsletter-ähnlichen Veröffentlichungen zum Verkauf an beteiligte Parteien.

[0278] Repackager **174** könnte beispielsweise einen Newsletter zu aktuellen politischen Fragen herausgeben sowie einen Essay von Autor **164** zur Veröffentlichung zusammen mit zwei weiteren Werken der Autoren **164a** und **164b** zur Veröffentlichung in der nächsten Newsletter-Ausgabe auswählen. Autoren **164**, **164a** und **164b** können Repackager **174** das Recht gewähren, das Werk umzuformatieren und weiter zu vertreiben. Dank dieses Umformatierungsrechts kann Repackager **174** die neueste Ausgabe des Newsletters erstellen und ihn sie einem sicheren elektronischen Container für den Gebrauch durch Kunde **95** vertreiben. In diesem Beispiel kann der sichere elektronische Container **152a** mindestens vier getrennt „gelieferte" Sätze von Geschäftsanforderungen enthalten, nämlich eine für jedes der drei Werke (wie jeweils durch Autor **164**, Autor **164a** und Autor **164b** vorgegeben) und eine für den Gesamt-Newsletter (wie durch Repackager **174** vorgegeben). Alternativ können die verschiedenen Werke und/oder die auf sie anwendbaren Steuermechanismen in unabhängigen sicheren Containern **152** versandt und geliefert werden, und/oder einige oder alle der Werke und/oder Steuermechanismen können rechnerfern hinterlegt werden.

[0279] Um den Newsletter zu lesen, öffnet Kunde **95** den elektronischen Container **152a**. Angenommen der Newsletter kostet (wie von Repackager **174** festgelegt) $ 10 pro Ausgabe. Die Zahlung oder Zahlungsermächtigung des Kunden in Höhe von $ 10 wird an Finanz-Clearinghaus **200** gesandt, das diese dergestalt zerlegt, dass jeder Wertketten-Teilnehmer entschädigt wird (beispielsweise kann Autor **164** $ 1, Herausgeber **168** $ 1, Aggregator **170** $ 50, jeder der zusätzlichen Autoren **164a** und **164b** $ 1 und Repackager **174** den Restbetrag erhalten, dies nach Maßgabe der anwendbaren elektronischen Steuermechanismen. Auf diese Weise kann Repackager für die Auswahl passender Artikel zum Thema und ihre Zusammenstellung in einer leserfreundlichen Veröffentlichung entschädigt werden, und er kann seine eigene Marke als Garant für die Gesamtqualität platzieren sowie seine selbst erstellten einmaligen Inhalte hinzufügen.

[0280] Fig. 28 zeigt ein Beispiel für „Superdistribution". Eine zentrale Sorge des Rechteinhabers sind Verletzungen des Urheberrechts durch „unberechtigte Weitergabe", d. h. illegale Vervielfältigung und Redistribution. Dieses Problem der unberechtigten Weitergabe ist in digitalen Umgebungen wie dem Internet ernst zu nehmen. Die in der Patentschrift von Ginter et al. offenbarte virtuelle Verteilungsumgebung und die in der vorliegenden Patentschrift offenbarten Anordnungen von Administrations- und Unterstützungsdiensten verwandeln die Weitergabe, ursprünglich eindeutig eine Bedrohung, in eine wichtige Chance. Wegen der eindeutigen, automatisierten, sicheren elektronischen Verwaltung von durch die virtuelle Verteilungsumgebung in der bevorzugten Ausführungsform bereitgestellten Wertkettenrechten kann der Verbraucher als ein vertrauenswürdiges Mitglied der Wertkette behandelt werden. Hierdurch wird ein

Superdistributions-Modell ermöglicht, in dem alle Kunden zu potentiellen Vertreibern werden. Da Erlöse aus Superdistribution nur minimale Rechteinhaberkosten mit sich bringen, stellt Superdistribution für Rechteinhaber an erfolgreichen Werken hohe Gewinnpotentiale bereit.

[0281] Angenommen, die Kundin **95** in Fig. 28 hat ein Werk von Aggregator **170** erhalten, das ihr so sehr gefällt, dass sie es an verschiedene Freunde und Kollegen weiterreichen will. Angenommen, Aggregator **170** hat Kunde **95** das Recht erteilt, das Werk weiter zu vertreiben – der Kunde kann nun einfach und problemlos eine Kopie des Werks an jeden beliebig vieler zusätzlicher potentieller Kunden **95(1)**... **95(N)** verschicken. Diese zusätzlichen Personen können Kundin **95** kennen und annehmen, dass diese ihnen nicht etwas zusenden würde, wäre dies nicht potentiell interessant und von hoher Qualität. Ferner können die nachgeschalteten Kunden in die Lage versetzt werden, zusammenfassende Informationen über das Werk zu lesen oder sich Auszüge aus ihm anzusehen (beispielsweise sich eine Vorschau vom Film anzusehen, das erste Kapitel eines Romans durchzulesen o. ä.), ohne damit eine Zahlung auszulösen.

[0282] Angenommen, sechs der nachgeschalteten Kunden **95(3)**-**95(8)** sind nach der kostenlosen Lektüre der Zusammenfassung oder der kostenlosen Betrachtung der ersten fünf Minuten des Films bereit, für die Inhalte beispielsweise jeweils $ 3,25 zu zahlen. Finanz-Clearinghaus **200** kann sicherstellen, dass Autor **164**, Herausgeber **168** und Aggregator **170** jeweils einen angemessen Anteil am Einkommen erhalten (beispielsweise der Autor $ 7, der Herausgeber $ 7 und der Aggregator $ 8,75).

[0283] Superdistribution ermöglicht eine beliebig große Anzahl Ebenen der Redistribution. Angenommen, drei der sechs nachgeschalteten Kunden **95(3)**-**95(8)** möchten das Werk beispielsweise an jeweils sechs weitere potentielle Kunden weiterreichen, so dass achtzehn zusätzliche Personen eine Kopie erhalten. Da die weiter vertriebenen Werke an konkrete Regelstrukturen gebunden sind, die eine einheitliche Zahlungsvereinbarung diktieren, erhalten Autor **164**, Herausgeber **168** und Aggregator **170** jeweils zusätzliche Zahlungen von jedem dieser neuen Kunden. Das Schneeballprinzip der Redistribution kann so über beliebig viele Verbraucher eine lange Zeit hinweg weiter betrieben werden und so die Erlöse bei minimalen Zusatzkosten für die Wertketten-Teilnehmer dramatisch steigern.

Zahlungsaggregation oder -bündelung

[0284] Mikrogebühren und Mikrozahlungen können zu einer wichtigen Basis für Transaktionen im Zusammenhang mit der Benutzung von Inhalten werden. Beispielsweise könnte eine Verbraucherin für jedes Mal zahlen, dass sie sich ein bestimmtes Werk ansieht oder ein bestimmtes Computerprogramm benutzt oder sich ein bestimmtes Musikstück anhört. Es können verschiedene Zahlungsvereinbarungen flexibel dergestalt bereitgestellt werden, dass der Verbraucher wählen kann, ob er eine höhere Einmalgebühr für den unbegrenzten Gebrauch oder kleinere Mikrozahlungen für jeden Gebrauch entrichten will. Ferner könnten Mikrozahlungen die am wenigsten lästige und die praktikabelste Methode sein, Commerce Utility Systeme **90** für ihre Dienste zu entschädigen. Die Möglichkeit, Mikrozahlungen effizient abzuwickeln, ist somit mit Hinblick auf die Unterstützung und Ermöglichung kleiner Forderungen sehr wichtig.

[0285] Traditionelle finanzielle Zahlungsmechanismen wie Kreditkarten, Schecks und dergleichen sind zur Abwicklung von Mikrozahlungen ungeeignet. Diese Systeme weisen typischerweise Kosten für Transaktionen in Bereichen auf, die für Geschäftsmodelle, welche auf vielen Käufen unter jeweils $ 5 basieren, eine große Belastung darstellen. Wenn beispielsweise die Abwicklung einer Zahlungs-Transaktion $ 0,50 kostet, werden Zahlungen unter einem bestimmten Betrag unwirtschaftlich, etwa pro Transaktion $ 2, da die Kosten der Zahlungsabwicklung hier einen wesentlichen Teil des Transaktionswerts ausmachen oder den eigentlichen Zahlbetrag gar übersteigen. Somit begünstigen traditionelle finanzielle Zahlungsmechanismen größere Einkäufe und bieten schlechte Bedingungen für Mikro-Einkäufe.

[0286] Fig. 29 zeigt, wie Zahlungsaggregation oder Bündelung dazu verwendet werden kann, diese Probleme zu umgehen, indem die Anzahl einzelner zu verrechnender Finanz-Transaktionen reduziert wird, und/oder indem der Umfang des für die Verrechnung solcher Transaktionen erforderlichen Datenaustauschs reduziert wird. Die exemplarische Zahlungsaggregation gemäß Fig. 29 kann im verbraucherseitigen elektronischen Gerät **100** innerhalb einer geschützten Verarbeitungsumgebung **154** stattfinden; oder in einem zentralisierten Finanz-Clearinghaus **200**; oder sie erfolgt teilweise im Gerät und teilweise im zentralisierten Clearinghaus. Dieser Vorgang der Zahlungsaggregation kann viele kleine Zahlungen zu größeren Zahlungen aggregieren oder kombinieren oder zu einem Bündel kleiner Zahlungen, die gleichzeitig abgewickelt werden können. Solche größeren Zahlungen und/oder Bündel können bei Bedarf periodisch zusammen mit anderen Transaktionsdaten gemeldet werden, um durch das Distributed Commerce Utility **75** abgeglichen und aufgezeichnet zu werden. Diese Möglichkeit, kleinere Zahlungen zu aggregieren, hat wichtige Vorteile mit Hinblick auf eine Erhöhung der Effizienz bei gleichzeitiger Reduzierung der Anzahl individueller zu verrechnender Transaktionen sowie einer Reduzierung des Datenübertragungs-Verkehrs im elektronischen Netzwerk

150. Freilich ist Zahlungsaggregation nicht unbedingt für jede Transaktion geeignet (große, kritische oder risikobehaftete Transaktionen können beispielsweise ein Clearing in Echtzeit erfordern), aber sie können in einer großen Anzahl von Routine-Transaktionen Anwendung finden, um die Commerce Utility Systeme **90** und das Gesamtsystem **50** zu entlasten. In einer Variante dieses Konzepts können bei der Zahlungsaggregation die einzelnen Beträge der individuellen Transaktionen erhalten werden, um ein hohes Maß an Detailliertheit bei der Berichterstattung zu ermöglichen, sie kann jedoch ausgelöst werden, wenn es zur Berichterstattung kommt (beispielsweise nach einem Einzug von X Dollar oder nach Y Transaktionen), sodass viele individuelle Transaktionen gebündelt und gemeinsam übertragen/verarbeitet werden können. Diese Form der Aggregation ist sinnvoll, wenn es darum geht, die Anzahl individueller, über das elektronische Netzwerk **150** transportierter Nachrichten und die Häufigkeit der Benachrichtigung zu reduzieren. In solchen Fällen kann das berichtende elektronische Gerät **100** über die folgenden Dinge Berichte erstellen: (I) über die aggregierten individuellen Transaktionen insgesamt oder (II) jede die individuellen Transaktionen oder (III) beides oder (IV) eine Kombination aus beidem.

[0287] Fig. 29 zeigt, dass ein Verbraucher sein elektronisches Gerät **100** für verschiedene Aktivitäten benutzen kann, wie beispielsweise die Lektüre eines Romans, die Betrachtung eines Videoprogramms, den Erwerb und die Überarbeitung von Forschungsergebnissen, indem er mit multimedialen Vorführungen interagiert und diese, sowie Finanzmanagement wie etwa Scheckbuch-Bilanzierung von zu Hause aus in Anspruch nimmt. Eine Mikrozahlung für jeden Gebrauch kann mit jeder dieser Aktivitäten in Beziehung gebracht werden. Beispielsweise könnte Verbraucher an Herausgeber A $ 1 und an Autor A $ 1,50 jedes Mal dann zahlen, wenn der Verbraucher auf eine elektronische Version eines Werks zugreift, das der Autor geschrieben und der Herausgeber vertrieben hat. Angenommen, die Werke von Autor A sind so populär geworden, dass sie verfilmt wurden. Der Verbraucher könnte für jeden Gebrauch einzeln bezahlen, wenn er sich einen dieser Filme ansieht, indem er an den Herausgeber A $ 5 zahlt, an den Autor A $ 3 und an das Distributed Commerce Utility 75 $ 0,50.

[0288] Zahlungsaggregatoren **266** (die bei Bedarf in der durch das verbraucherseitige elektronische Gerät **100** bereitgestellten geschützten Verarbeitungsumgebung **154** am Verbraucherstandort betrieben werden können) können Zahlungen zu gemeinsamen Größen aggregieren und hierbei eine laufende Summe des Geldbetrags, der dem Herausgeber A geschuldet ist, des Geldbetrags, der Autor A geschuldet ist sowie des Geldbetrags, der dem Distributed Commerce Utility **75** geschuldet ist, einbehalten. Diese laufende Summe kann jedes Mal, wenn der Verbraucher ein weiteres Zahlungsereignis auslöst, inkrementiert werden. Die aggregierten Zahlungsbeträge können auf Grundlage bestimmter Zeitintervalle (beispielsweise wöchentlich, monatlich oder täglich), des Eintreffens bestimmter Ereignisse (beispielsweise die Verbraucherin hat ihre Kreditgenehmigung überschritten und benötigt eine neue, bestimmte elektronische Steuermechanismen sind ausgelaufen etc.) und/oder einer Mischform einzelner oder aller dieser Techniken periodisch oder anderweitig an Finanz-Clearinghaus **200** oder andere Commerce Utility Systeme **90** gemeldet werden.

[0289] Fig. 30 zeigt ein weiteres Beispiel einer Zahlungsaggregation über einige Verbraucher-Transaktionen. In diesem Beispiel werden Zahlungen an ein und dieselben Wertketten-Teilnehmer unter Verwendung ein und derselben Zahlungsmethode zu Gesamtbeträgen aggregiert. Durch diese Zahlungsaggregation, die am Standort des Verbrauchers und/oder in einem Finanz-Clearinghaus stattfinden kann, lässt sich die Gesamtzahl der zu verrechnenden Finanz-Transaktionen reduzieren. Hierdurch werden Effizienz und Durchsatz gesteigert und die Kosten für die Abwicklung der individuellen Verbraucher-Transaktionen gesenkt.

[0290] Fig. 31 zeigt noch ein weiteres Beispiel für Zahlungsaggregation, in dem die Aggregation über Transaktionen mehrerer verschiedener Verbraucher erfolgt. Beispielsweise könnten sämtliche zu einem bestimmten Anbieter gehörigen Transaktionen unter Verwendung einer bestimmten Zahlungsmethode von einem Finanz-Clearinghaus **200** aggregiert werden. Wichtig ist, dass die Zahlungsaggregations-Techniken gemäß Fig. 29-Fig. 31 nicht zwangsläufig zu einem Verlust an Detailliertheit der einzelnen Transaktion führen. Somit können die verbraucherseitigen elektronischen Geräte **100** dennoch detaillierte Informationen über jede einzelne Transaktion aufzeichnen und melden, und Finanz-Clearinghaus **200** und/oder Usage-Clearinghaus **300** können detaillierte Benutzungsdaten für jede einzelne Transaktion melden, und zwar auch dann, wenn die einzelnen Transaktions-Zahlungen mit dem Ziel einer effizienteren Zahlungsverarbeitung und -abwicklung zusammengefasst werden. Diese Möglichkeit, detailliertere und feiner granulierte Benutzungsdaten getrennt abzuwickeln und zu verarbeiten und gleichzeitig Zahlungen zu aggregieren, kann einen hohen Grad an Nachvollziehbarkeit der Audits bereitstellen, ohne den Mechanismus der Zahlungsabwicklung über Gebühr zu belasten. In einigen Fällen führt der Verlust detaillierter Aufzeichnungen zu Einsparungen seitens des Clearinghauses. Sie können verworfen werden, aber ihre Aufbewahrung im benutzerseitigen System und/oder im Repositor eines Commerce Utility Systems **90** bietet auch Vorteile. Kommt es zu Meinungsverschiedenheiten bezüglich der Rech-

nung, so könnte sich beispielsweise die lokale Kopie der detaillierten Aufzeichnungen als nützlicher Beleg darüber erweisen, was tatsächlich geschehen ist, selbst wenn diese Aufzeichnungen nie an das Clearinghaus übermittelt wurden.

[0291] Fig. 32 zeigt, wie ein exemplarisches Finanz-Clearinghaus **200** modifiziert werden könnte, um eine Zahlungsaggregator-Komponente **268** zu beherbergen. Zahlungsaggregator **268** könnte dafür eingesetzt werden, von mehreren verschiedenen verbraucherseitigen elektronischen Geräten **100** oder anderen Quellen eintreffende Zahlungen zu aggregieren, und diese aggregierten Zahlungen zur Abwicklung beispielsweise über dritte Abwicklungsdienste an Weiche **200** zu übergeben. Zahlungsaggregator **268** kann ggf. auch nur ausgewählte Zahlungen aggregieren, während er andere Zahlungen für eine direkte Abwicklung ohne Aggregation an Weiche **200** passieren lässt. Zahlungsaggregation kann auf mehreren verschiedenen Faktoren aufbauen. So können Zahlungen auf der Grundlage solcher Faktoren wie etwa Verbraucher, Anbieter, Zahlungsmethode oder einer Kombination aus beliebigen oder allen dieser Faktoren aggregiert werden. Diese Aggregationsfunktion kann vollständig oder teilweise in den elektronischen Geräten von Verbraucher **95** ausgeführt werden, oder sie könnten zentral durch ein zentralisiertes Clearinghaus **200** ausgeführt werden.

Usage-Clearinghaus **300**

[0292] Fig. 33 zeigt ein Beispiel für ein Commerce Utility System **300** vom Typ eines Usage-Clearinghauses. Die Dienste und Funktionen von Usage-Clearinghäusern können allgemein detaillierte, zusammengefasste und/oder abgeleitete Benutzungsdaten über die Benutzung und/oder Ausführung digitaler Eigenschaften und/oder digitaler Prozesse erfassen, analysieren und „umfunktionieren". Diese Informationen können beliebige Informationen umfassen, die Aufschluss über elektronische Transaktions-Aktivitäten geben. Usage-Clearinghäuser und/oder Unterstützungsdienste können beispielsweise folgendes bereitstellen und/oder erleichtern:

- Unabhängiges Auditing und unabhängige Berichterstattung (die unabhängig von Clearingdiensten für finanzielle Abwicklung angeboten können);
- allgemeine Markfforschung;
- Aushandeln, Implementieren, Bestimmen und Übermitteln von Datenschutz- und Vertraulichkeitsebenen mit Kunden und Teilnehmern der Wertkette in Bezug auf solche Benutzungsdaten; und
- Kundenindividuelles Marketing und Verkauf, Vermietung oder Lizenzierung konsolidierter Listen.

[0293] Genauer können Usage-Clearing-Dienste in Übereinstimmung mit den vorliegenden Erfindungen beispielsweise eine beliebige Kombination aus den nachstehend detaillierten Merkmalen und/oder -funktionen bereitstellen:

- Kompilation, Aggregation, Benutzung, Gewinnung und/oder Bereitstellung von Informationen, die über die Benutzung eines sicheren Containers (sicherer Container), von Inhalten sicherer Container und/oder von beliebigen anderen Inhalten und/oder beliebigen digitalen Regelabläufen Aufschluss geben und/oder anderweitig mit diesen in Zusammenhang stehen, wobei solche Informationen (a) einen oder mehrere Benutzer von Inhalten und/oder Abläufen, (b) eine oder mehrere Klassen von Inhalten, Regelabläufen, die Benutzung von Inhalten und/oder Benutzer und/oder (c) einen oder mehrere Empfänger solcher Benutzungsdaten beschreiben und/oder anderweitig mit diesen in Zusammenhang stehen.
- Ermöglichung der Kontrolle und Meldung von Informationen über Inhalte und/oder die Benutzung von Prozesssteuerung und/oder Verarbeitungsdaten in hochgranularer (beispielsweise detaillierter) Form.
- Kann Benutzungsdaten erfassen, aggregieren, analysieren, zusammenfassen, extrahieren, melden, vertreiben, vermieten, lizenzieren und/oder verkaufen.
- Nutzbarmachung von Informationen, die aus dem Benutzerkontakt mit Inhalten wie Werbung, Informationsmaterialien, Unterhaltung, Schulungsmaterialien, Produktivitätssoftware-Anwendungen von Unternehmen etc. gewonnen wurden und sichere Lieferung mindestens eines Teils der so gewonnenen Informationen und/oder verwandten Informationen durch den Einsatz von VDE-Mechanismen in der bevorzugten Ausführungsform an Benutzungsdaten aggregierende und/oder analysierende Clearinghäuser, wobei ein solches Clearinghaus sicher mindestens einen Teil dieser aus solchen Informationen gewonnenen Benutzungsdaten oder Informationen für mindestens ein weiteres Clearinghaus und/oder einen weiteren Rechteinhaber der Wertkette bereitstellt; und wobei dieses Clearinghaus unterschiedliche gewonnene Benutzungsdaten an unterschiedliche solche andere Parteien sicher bereitstellen kann, die die Rolle eines Clearinghauses oder eines anderen Rechteinhabers ausfüllen.
- Verwendung der „Information-Exhaust"-Prüfketten, die von Zählmechanismen der geschützten Verarbeitungsumgebung des Benutzers erstellt und/oder von diesen gewonnen wurden, auf der Grundlage verschiedener Techniken (beispielsweise der in Ginter et al. offenbarten).
- Möglichkeit, detaillierte Benutzungsdaten zu erfassen und zu analysieren, zum Beispiel, wie oft eine digitale Eigenschaft bzw. ein beliebiger Teil einer Eigenschaft geöffnet, ausschnittsweise ver-

wendet, eingebettet oder ausgeführt wurde, oder wie lange ein Wertketten-Teilnehmer eine Eigenschaft wie ein interaktives Spiel oder eine Multimediavorführung, Computersoftware oder Module oder Teile solcher Produkte benutzt hat.

• Bereitstellung verschiedener Umwidmungs-Möglichkeiten für von Verbrauchern oder anderen sicheren geschützten Verarbeitungsumgebungen eintreffende Benutzungsinformationen.

• Bereitstellung von unabhängigen Auditing-Eigenschaften durch Dritte, nützlich etwa für die Archivierung und Nichtzurückweisung.

• Bereitstellung von Informationen auf der Grundlage von Usage Auditing, Benutzerprofil-Erstellung und/oder Marktuntersuchung in Bezug auf die Benutzung eines oder mehrerer sicherer Container und/oder Inhalte und/oder VDE-verwalteter Prozesssteuerung in der bevorzugten Ausführungsform.

• Bereitstellung von neutralen, vertrauenswürdigen Usage-Aggregation- und Usage-Berichterstattungs-Diensten durch Audits von Dritten für Rechteinhaber, Verbraucher und/oder andere Teilnehmer der Wertkette und/oder beteiligte Parteien wie staatliche Einrichtungen (Informationen für Steuerzwecke, für die Durchsetzung von Gesetzen, für Marktforschungszwecke, statistische Zwecke etc.).

• Bereitstellung von Audit-Eigenschaften in Verbindung mit Rechte- und Berechtigungs-Clearing von Regeln und Steuermechanismen (beispielsweise einen Bericht darüber bereitstellen, welche Berechtigungen und Rechte für Regeln und Steuermechanismen ausgeübt wurden, beispielsweise durch wen, wofür und wann, womit tatsächliche Benutzer-Aktivitäten an bestimmte Muster von Berechtigungen und Rechten und/oder Regeln und Steuermechanismen gekoppelt werden).

• In der bevorzugten Ausführungsform Bereitstellung standardisierter und kundenindividueller Berichterstattung und Analysen auf der Grundlage VDE-basierter Regeln und Steuermechanismen, produziert und geliefert in VDE-Containern an alle und/oder eine beliebige oder mehrere Gruppierungen von Inhaltserstellern, Inhaltsvertreibern, Industrieanalysten, Wirtschaftsverbänden und beliebigen anderen Interessengruppen und Teilnehmern der Wertkette und/oder beliebigen anderen beteiligten Parteien wie staatliche Statistiker, Regler und/oder Finanzämter.

• Belieferung mit Daten in einer beliebigen Kombination aus unbearbeiteten, bearbeiteten, zusammengefassten, erworbenen und aggregierten vertrauenswürdigen Daten zur Unterstützung mehrerer Geschäftsmodelle innerhalb einer beliebigen Wertkette und/oder über Wertkettengrenzen hinweg und/oder in mehreren Wertketten.

• Die Verteilung von Benutzungsdaten getrennt von und/oder zusammen mit Clearingdiensten der finanzielle Abwicklung an Teilnehmer der Wertkette und andere Parteien innerhalb oder außerhalb der elektronischen Gemeinschaft.

• Unterstützung von Steuermechanismen zur Wahrung des Datenschutzes und der Vertraulichkeit dergestalt, dass die Rechte und Interessen aller Teilnehmer der Wertkette in Bezug auf Benutzungsdaten vollständig geschützt sind wie beispielsweise solche Rechte, die mittels VDE-Ketten der Verarbeitung und Steuerung verwalteten Geschäftsmodellen eigen sind.

• Kann Datenschutzanforderungen Rechnung tragen, beispielsweise dahingehend, dass nicht mehr Informationen offen gelegt werden, als wofür seitens eines Verbrauchers oder Anbieters von Inhalten einer Wertkette, eines Aggregators, Umwidmers oder eines anderen Benutzers eines elektronischen Geräts, das in der bevorzugten Ausführungsform für eine sichere, verwaltete Inhaltskontrolle oder andere Prozesssteuerung VDE verwendet, eine Vollmacht erteilt wird, und beispielsweise ein solcher bevollmächtigender Benutzer darüber informiert wird, welche Art von Informationen erfasst und/oder verrechnet werden).

• Kann zumindest teilweise auf der Grundlage von Regeln und Steuermechanismen auf vertrauenswürdige Weise einen oder mehrere Teil(e) vertraulicher oder geschützter Benutzungsdaten automatisch verbergen (beispielsweise verschlüsseln), entfernen und/oder umwandeln, bevor solche Informationen weiterverarbeitet werden, bzw. bevor solche Informationen an eine beliebige oder mehrere zusätzliche Parteien einschließlich eines beliebigen weiteren Usage-Clearinghauses (beliebiger weiterer Clearinghäuser) geliefert werden, wobei Datenschutz und Vertraulichkeit einschließlich Geschäftsgeheimnisse effizient geschützt werden.

• Schutz von Kerninformationen über das Geschäftsmodell vor Datendiebstahl durch andere beteiligte Parteien und/oder vor unbeabsichtigter Offenlegung gegenüber anderen beteiligten Parteien und/oder der Öffentlichkeit, womit eine Grundlage für wirklich vertrauenswürdige kommerzielle Netzwerke gelegt ist.

• Ausstattung von Teilnehmern einer Wertkette wie beispielsweise kommerziellen Herausgebern und Vertreibern und/oder Verbrauchern und Anbieterunternehmen von Dienstleistungen und/oder Produkten mit der Möglichkeit, die Detailliertheit der an einen beliebigen Rechteinhaber der Wertkette zu übermittelnden Benutzungsdaten auszuhandeln, wobei eine solche Detailliertheit je in Abhängigkeit davon differieren kann, wer der Empfänger dieser Informationen ist, und welcher konkreter Typ und/oder Subtyp Benutzungsdaten weitergegeben wird, wobei mehrere unterschiedliche Detailliertheitsgrade für unterschiedliche Teilmengen solcher Benutzungsdaten einem bestimmten Empfänger von Benutzungsdaten

und/oder als ein bestimmter Lieferposten bereitgestellt werden können, wobei eine Bestimmung der Detailliertheit zumindest teilweise durch die Rechte einer bestimmten Partei bestimmt wird wie zumindest teilweise durch Informationen der VDE-Regeln und -Steuermechanismen in der bevorzugten Ausführungsform beschrieben.

• Ausstattung von Verbrauchern und Organisationen mit der Möglichkeit, den Detailliertheitsgrad der an die Rechteinhaber einer Wertkette übermittelten Informationen auszuhandeln.

• Ausstattung von Verbrauchern oder anderen Teilnehmern der Wertkette wie Erstellern, Herausgebern, Vertreibern und Umwidmern mit der Möglichkeit, den Grad (die Grade) der Detailliertheit, Aggregation und/oder Anonymität vorzugeben und/oder auszuhandeln, die sie in Bezug auf die Benutzungsdaten hinsichtlich ihrer Benutzung eines bestimmten Inhalts, einer bestimmten Inhaltsklasse, eines bestimmten Vorgangs, einer bestimmten Vorgangklasse und/oder Zahlungsanforderungen wünschen (beispielsweise kann Anonymität und/oder Aufrechterhaltung des Datenschutzes in Bezug auf einige oder alle Benutzungsdetails eine Zahlungsprämie erfordern, die den Verlust einer solchen Information ausgleicht).

• Ausstattung von Verbrauchern von Informationen und/oder andere Teilnehmern der Wertkette mit der Möglichkeit, ihr „Information-Exhaust" kundenindividuell zu gestalten und Regeln und Steuermechanismen darüber festzulegen, wie sie ihre Benutzungsdaten aggregiert oder anderweitig verwendet sehen wollen, dies unter Beachtung der konkurrierenden Bedürfnissen der Rechteinhaber, Informationen zu erhalten, die zu erhalten sie berechtigt sind und/oder Informationen zu erhalten, von denen der Benutzer und der Rechteinhaber auf elektronischem Wege einvernehmlich vereinbaren, dass diese dem Rechteinhaber zur Verfügung gestellt werden können. Benutzer und/oder ein oder mehrere Rechteinhaber können das Recht haben, Grenzen für Benutzungsdaten vorzugeben (beispielsweise VDE-Kette der Verarbeitung und Steuerung benutzen) und/oder bestimmte Benutzungsdaten zu beschreiben, die an einen oder mehrere andere Rechteinhaber geliefert werden können oder müssen.

• Unterstützung einer maßgeblichen Kontrolle des Wertketten-Teilnehmers darüber, welche Art Benutzungsdaten über den Wertketten-Teilnehmer akkumuliert wird, wer auf welche Informationen zugreifen kann, und wie solche Informationen verwendet werden können, wie solche Informationen gewonnen und verarbeitet werden sowie der Grad, zu dem Benutzungsaufzeichnungen an einen bestimmten Wertketten-Teilnehmer bzw. an eine bestimmte Organisation gekoppelt werden.

• Sichere Benutzung von Containern (beispielsweise unter Verwendung sicherer VDE-Container in Kombination mit einer geschützten VDE-Verarbeitungsumgebung und Möglichkeiten eines sicheren Datenverkehrs wie beschrieben in Ginter et al.) bei jedem Schritt, Teil und/oder Vorgang der Bereitstellung sicherer Usage-Clearingdienste.

• Unterstützung einer Bereitstellung von Nachlässen, Zuschüssen und/oder Gutscheinen für Teilnehmer der Wertkette wie etwa Verbraucher, Händler, Umwidmer (Repurposer) etc. als Gegenleistung für Benutzungsdaten oder feiner granulierte Benutzungsdaten (beispielsweise bei gleichzeitiger Verbesserung des Datenschutzes in bestimmter Hinsicht).

• Erstellung von und Versorgung beteiligter Parteien mit Marktforschung und Berichterstattung und konsolidierten Marketinglisten (für gezielten Versand von Mails, Direktverkauf und andere Formen gezielten Marketings). Solche Materialien zeigen allgemeine Analogien zu unabhängigen Audits über Auflagen von Zeitschriften und Zeitungen, Berichte über Ratings durch das Fernsehpublikum und/oder kommerzielle Listen für gezieltes Marketing, werden jedoch in einer hocheffizienten, verteilten und sicheren elektronischen Umgebung generiert. Solche Materialien können bei Bedarf mit wichtigen neuen Detailformen (beispielsweise Ansicht, Ausdruck, Extrahierung, Wiederverwendung, elektronische Speicherung, Umverteilung etc.) mit deutliche stärkerer Granulierung der Informationen ausgestattet werden sowie mit kundenindividueller selektiver Übergabe von Materialien auf der Grundlage von Anforderungen durch die Empfänger, Zahlungen, Rechten und/oder Interessenkonflikten mit einer oder mehreren Parteien, die als Rechteinhaber an einem oder mehreren Teilen der zugrunde liegenden Informationen interessiert sind.

• Benutzung detaillierter Benutzungsdaten für die automatische Erstellung von Klassifikationshierarchien, Anordnungen, Gruppen und/oder Klassen sowie die automatische Zuordnung von Individuen, Gruppen von Individuen, Organisationen, Gruppen von Organisationen, digitalen und/oder analogen Inhalten oder Gruppen digitaler und/oder analoger Inhalte zu einer oder mehreren Klassen, die auf der Grundlage von Benutzungsdaten aufgestellt wurden, welche in Verbindung mit mindestens einem sicheren Container und/oder einer VDE in der bevorzugten Ausführungsform erstellt, erfasst, übertragen wurden.

• Unterstützung von Werbung und Marketing einschließlich der Unterstützung einer effizienten Wertkettenautomatisierung bei der Belieferung mit solchen Diensten wie automatische Auswahl des Empfängers von Werbung oder automatische Lieferung von Werbung und/oder anderen Marketingmaterialien an definierte Sätze (beispielsweise eine oder mehrere Klassen) von Verbrauchern, Fachleuten, Angestellten und Unternehmen, wobei die Sätze mittels Eigenauswahl, Benutzungsdaten, Benutzungsdatenprofile oder durch ein be-

liebiges anderes Mittel definiert sein können, wobei diese Sätze aus einem beliebigen oder mehreren Teilnehmern der Wertkette (beispielsweise aus Erstellern, Verbrauchern, Vertreibern, Dienstleistern, Websites, verteilten Clearinghäusern) zusammengesetzt sein können, wobei dieser) eine oder mehreren Teilnehmer unterschiedliche, speziell zugeschnittene Materialien empfangen können, wobei diese empfangenden Teilnehmer solche Materialien neu vertreiben können, sofern sie durch die Regeln und Steuermechanismen autorisiert sind, wobei solche Teilnehmer eine Gutschrift, Gutscheine, eine Geldzahlung und/oder andere Formen der Gegenleistung für eine solche Redistribution erhalten können, wobei eine solche Redistribution so aussehen kann, dass einige oder alle der so erhaltenen Materialien einer oder mehreren anderen Parteien zumindest teilweise auf der Grundlage von Eigenauswahl, Benutzungsdaten, Benutzungsdatenprofilen oder durch ein beliebiges anderes Mittel zugeleitet werden können, wobei alle solche Abläufe durch eine VDE-Kette der Verarbeitung und Steuerung zwischen Knoten in der bevorzugten Ausführungsform sicher verwaltet (beispielsweise unterstützt) werden können.

• Festlegung der dem Rechteinhaber vom Werbetreibenden zustehenden Zahlungen und/oder anderen Gegenleistungen auf der Grundlage des Kontaktes eines Benutzers der Wertkette mit Werbeinhalten bei zumindest teilweiser sicherer Automatisierung der Verteilung von Teilen einer solchen Gegenleistung auf mehrere Rechteinhaber, die in Bezug auf solche Inhalte und/oder Abläufe beteiligt sind, die als Grundlage für die Festlegung einer solchen Gegenleistung dienten.

• Unterstützung einer überragenden gezielten Marktsegmentierung und der Gestaltung besser zugeschnittener Informationsprodukte und Geschäftsmodelle auf der Grundlage direkter, spezifischerer und detaillierterer Benutzungsdaten sowie auf der Grundlage von Präferenzen der Kunden und der Wertkette, die in Benutzungsdaten, Benutzerprofilen, Identifikationsdaten über Klassen etc. implizit enthalten sind, die dort explizit genannt werden und/oder aus diesen automatisch gewonnen werden.

• Ermöglichung „privater" Usage-Clearinghäuser (ein Usage-Clearinghaus, das durch eine Organisation gesteuert und/oder betrieben wird), um bestimmte detaillierte Benutzungsinformationen zu gewinnen, wobei solche Usage-Clearinghäuser Benutzungsanalysen und/oder eine andere Verarbeitung solcher Informationen ausführen und selektiv beschränkte Benutzungsinformationen (beispielsweise unter Verwendung von Abstraktionen höherer Ebene, zusammengefasster Informationen, Beschränkungen für und/oder Art der Benutzung von Benutzungsdaten – Betrachten, Ausdrucken, Abspeichern, Umverteilung etc.) für einige oder alle solcher Benutzungsdaten an stärker zentralisiertere Clearinghäuser und/oder Clearinghäuser anderer Parteien und/oder anderer Teilnehmer der Wertkette bereitstellen können, wobei auf aus der Benutzung unterschiedlicher Klassen von Inhalten, Abläufen, Benutzern und/oder Benutzergruppen gewonnene Benutzungsdaten unterschiedliche Beschränkungen für solche Benutzungsdaten angewandt werden können, wobei solche Beschränkungsmöglichkeiten einen wichtigen zusätzlichen Schutz vertraulicher Informationen mit Geschäftsgeheimnischarakter eines Unternehmens oder einer anderen Organisation dadurch bereitstellen, das die Detailliertheit bestimmter interner Aktivitäten verdeckt wird, wobei eine oder mehrere andere Parteien einer Wertkette eine Zahlung und/oder andere Gegenleistung für die Zurückhaltung solcher detaillierter Benutzungsdaten einfordern können.

• Ausstattung von Organisationen mit der Möglichkeit, Clearinghäuser für private Benutzungsdaten in Intranets von Unternehmen zu betreiben, wobei solche Clearinghäuser in den Dokumenten-Workflow und/oder in die datenlogistischen Systeme des Unternehmens integriert sind.

• Mit Clearinghäusern für Organisationen privater Benutzung (beispielsweise Firma, Behörde, Personengesellschaft oder eine beliebige andere organisierte betriebliche Einheit) Empfang von Benutzungsdaten von elektronischen Geräten innerhalb der Organisation und Aggregation von Aufzeichnungen in detaillierte Berichte für den internen Gebrauch und/oder die Übergabe unbearbeiteter detaillierter Daten für den internen Gebrauch, wobei jedoch lediglich Benutzungsdaten in Kurzberichte für die externe Verteilung beispielsweise auf Rechteinhaber und/oder andere Teilnehmer der Wertkette und/oder ein oder mehrere kommerzielle Clearinghäuser aggregiert werden, wobei detaillierte Daten für den internen Gebrauch in der bevorzugten Ausführungsform als VDE-geschützter Inhalt geschützt sind, und der Zugriff auf solche Inhalte bzw. ein anderer Gebrauch solcher Inhalte auf die vorgegeben Parteien und/oder auf die vorgegebene Weise beschränkt ist, dies zumindest teilweise auf Grundlage der sicher aufrecht erhaltenen elektronischen Identität der vorgegebenen Parteien wie beispielsweise beliebige relevante Identifikationsdaten über die Klasse einer Partei (beispielsweise Mitglied einer bestimmten Forschungsgruppe, Geschäftsführer), die diesbezüglich über bestimmte Privilegien bei der Benutzung von Informationen verfügt.

• Identifikation und – über private Usage-Clearinghäuser – Zustellung benutzungsbezogener Informationen, die wichtige und wertvolle Benutzungsdaten für die Zuweisung organisationsinterner Ressourcen, für die Ausrichtung der Forschung und für andere wichtige geschäftliche Zwecke be-

reitstellen.
• Verteilung des Usage Clearing (beispielsweise aus Gründen der Effizienz und/oder aus anderen Gründen).
• Verteilung von Funktionen des Usage Clearing über ein Netzwerk oder ein anderes System (beispielsweise jeder Verbraucher- und/oder anderer Wertkettenteilnehmer-Knoten ist potentiell ein verteilter Usage-Clearing-Dienst, der zumindest teilweise sein eigenes sicheres Usage Clearing auslöst, wobei ein solcher Teilnehmerknoten Benutzungsdaten direkt an einen oder mehrere andere Teilnehmer übermitteln kann) sowie – in der bevorzugten Ausführungsform – in Übereinstimmung mit den Regeln und Steuermechanismen und anderen VDE-Techniken wie in der Patentschrift von Ginter et al. beschrieben.
• Hierarchische Organisation von Usage-Clearinghäusern, zumindest teilweise, um die Vertraulichkeit auf jeder Hierarchieebene zu schützen.
• Erteilung von Vollmachten und/oder Bereitstellung von Diensten für oder in Verbindung mit einem oder mehreren verteilten untergeordneten Usage-Clearinghäusern, deren Vorgänge logisch und/oder physisch anderenorts stattfinden können, wie etwa innerhalb eines Unternehmens oder einer Behörde und/oder in einer oder mehreren Gerichtsbarkeit(en), und/oder die Teilbereiche der geschäftlichen Gesamttätigkeit eines übergeordneten Usage-Clearinghauses abdecken.
• Verteilung und/oder die anderweitige Autorisierung von Funktionen des Usage Clearing in einem System oder Netzwerk, wobei beispielsweise jeder Verbraucher und/oder ein bestimmter oder alle anderen geschützten Verarbeitungsumgebungen (Knoten) eines Wertketten-Teilnehmers potentiell einen verteilten Usage-Clearing-Dienst unterstützen und in der Umgebung des übergreifenden Distributed Commerce Utilitys arbeiten können.
• Auslösen der eigenen sicheren Transaktionen des Usage Clearing direkt mit einem oder mehreren anderen Teilnehmern.
• Bereitstellung eines interoperablen Betriebs mit einem oder mehreren interoperablen Knoten anderer Teilnehmer unter Verwendung jeder oder aller solcher Aktivitäten, die auf Techniken einer virtuellen Verteilungsumgebung zurückgreifen.
• Benutzung eines Clearinghauses, um Benutzungsdaten zu generieren, die zumindest teilweise bei der Gestaltung und/oder Vermarktung von Produkten und/oder Dienstleistungen in Bezug auf solche Produkte und/oder Dienstleistungen benutzt werden, deren Benutzung durch solche Benutzungsdaten beschrieben wird.
• Kann hierarchisch, nach dem Peer-to-Peer-Prinzp oder in einer Kombination aus beidem organisiert werden, wobei die Verantwortung für das Usage Clearing für unterschiedliche Handelsmodelle und/oder Aktivitäten und/oder Wertketten auf verschiedene Art und Weise verteilt werden kann, wobei eine oder mehrere bestimmte Parteien gegenüber anderen Parteien beispielsweise in einer oder mehrerer Hinsicht hierarchisch übergeordnet, und in einer oder mehrerer anderer Hinsicht hierarchisch ein Peer oder untergeordnet sein kann, das heißt, die Beziehung unter den Teilnehmern ist programmierbar und kann dergestalt eingestellt (und nachträglich) verändert werden, dass eine oder mehrere gewünschte Anordnungen des Usage Clearings für bestimmte gewerbliche Tätigkeiten, Wertketten oder Modelle hergestellt werden.

[0294] Fig. 33 zeigt ein Beispiel für ein Usage-Clearinghaus **300** aus Verarbeitungssicht. Usage-Clearinghaus **300** erfasst, analysiert und meldet in diesem Beispiel die Benutzung digitaler Informationen einschließlich, aber nicht beschränkt auf die Benutzung digitaler Inhalte. Usage-Clearinghaus **300** erfüllt in diesem Beispiel die folgenden Funktionen:
- Datenerfassung **314**,
- Datenbankverwaltung **316**,
- Datenschutzkontrolle **318**,
- Sicheres Auditing **320**,
- Sichere Berichterstattung **322**,
- Datenaggregation **324**,
- Werbung und Marketing **326**,
- Benutzungsanalyse **328**,
- Replikation **330**, und
- Propagierung **332**.

[0295] Bei Bedarf kann der Datenaustausch zwischen Usage-Clearinghaus **300** und anderen elektronischen Geräten **100** in sicheren elektronischen Containern **152** erfolgen. Wie in Verbindung mit Finanz-Clearinghaus **200** genauer erklärt, kann auch Usage-Clearinghaus **300** die Container in Echtzeit und/oder asynchron empfangen. Im Usage-Clearinghaus **300** kann die Echtzeit-Anforderung Werbe- oder Ratingdaten umfassen, die einige oder alle ihrer Werte mit zeitlicher Funktion verlieren (werden beispielsweise gewisse Ratingdaten nicht binnen einer bestimmten Zeit geliefert, so verlieren diese möglicherweise in einer bestimmten Marktanalyse an Relevanz; oder wenn Werbetreibende Benutzungsdaten nicht sofort erhalten, können sie nicht so effektiv auf den Kundengeschmack reagieren). In einem weiteren Fall kann die Lieferung von Benutzungsdaten erforderlich sein (beispielsweise ein Benutzer kehrt vom Urlaub zurück und stellt fest, das sein erforderliches Audit-Datum und die Nachfrist ausgelaufen sind, und die Benutzung einer bestimmten Eigenschaft ist erst nach Abschluss des Audits wieder möglich). Eine asynchrone Lieferung ist aus denselben Gründen wie oben in Verbindung mit Finanz-Clearinghaus **200** beschrieben in einigen Fällen immer noch vorzuziehen.

[0296] Die Datenerfassungsfunktion **314** dient da-

zu, Benutzungsaufzeichnungen **302** zusätzlich zu anderen Informationstypen wie Regeln und Steuermechanismen **188** (welche Informationen beispielsweise zu Preisen und Berechtigungen bereitstellen können), Bilanzabschlüsse **240a**, detaillierte Finanzberichte **240b**, und Anforderungen von Benutzungsdaten und/oder -analysen **336** zu erfassen. Die Datenerfassungsfunktion **314** kann eng mit der Datenbankverwaltungsfunktion **316** interagieren, wobei verschiedene Informationstypen in einer Benutzungsdatenbank oder in einer anderen Datenbank gespeichert und geführt werden können. Die Replikations- und Propagierungsfunktionen **330**, **332** können dazu verwendet werden, die Inhalte von Datenbank **316** mit anderen (beispielsweise durch andere Usage-Clearinghäuser **300** unterhaltene) Datenbanken zu synchronisieren und/oder dazu, in einer Anzahl sicherer Netzwerke geschützter Verarbeitungsumgebungen oder elektronischer Geräte eine verteilte Datenbank bereitzustellen.

[0297] Datenaggregation **324** und -analyse **328** kann dazu verwendet werden, die Inhalte der durch die Datenauswahlfunktion **314** erfassten und/oder in der Datenbank **316** abgespeicherten Daten zu analysieren, wodurch Usage-Clearinghaus **300** in die Lage versetzt wird, Auditing **320** und/oder Berichterstattung **322** durchzuführen. Datenschutzkontrolle **318** kann in Verbindung mit der Berichterstattungsfunktion **322** verwendet werden, um Dritten gegenüber nur bestimmte und keine anderen Informationen offen zu legen, wodurch die Datenschutz- und Vertraulichkeitsinteressen jenes Verbrauchers geschützt werden, für den Benutzungsdaten gesammelt wurden. Die hierfür anstehende Steuerung **316** kann in Regeln ausgedrückt werden, denen der Container unterliegt, in dem die Informationen zugestellt wurden.

[0298] Die Berichterstattungsfunktion **322** kann verschiedene Usage-Auditing-Berichte **304** generieren. Ferner kann Usage-Clearinghaus **300** dazu verwendet werden, um Werbungs- und/oder Marketingunterstützung **326** bereitzustellen (beispielsweise um zu einer gezielten Werbung für demographisch passende Verbraucher beizutragen, und/oder um Markt- und Werbeforschung bereitzustellen). Auf diese Weise, kann in einem Beispiel Usage-Clearinghaus **300** selbst Werbung **340** zur Betrachtung durch gezielt ausgewählte Verbraucher produzieren und/oder vertreiben oder solche Werbung im Namen anderer zu liefern. Usage-Clearinghaus **300** kann überdies Informationsanforderungen **336** mit von ihm generierten kundenspezifischen Antworten **342** beantworten, ferner kann es Freigabesignale **344** generieren, die elektronische Geräte **100** dazu bevollmächtigen, die Benutzungsdaten aus lokalen Datenbanken zu löschen und/oder als „erledigt" zu markieren, sobald die betreffenden Audit-Aufzeichnungen an Usage-Clearinghaus **300** übermittelt, und dieser Transfer bestätigt wurden. Verbraucher **95** kann möglicherweise daran interessiert sein, dass diese Benutzungsinformationen nach ihrer „Freigabe" aufbewahrt und nicht gelöscht werden (beispielsweise aus Neugierde, um mehr über das Verhalten anderer (Angestellter, Kinder etc.) zu erfahren).

[0299] Usage-Clearinghaus **300** kann seine eigenen Steuermechanismen **188b** generieren, um beispielsweise zu regeln, wie Benutzungsdaten, Marktanalysedaten oder andere Daten durch andere benutzt werden können. So könnte Usage-Clearinghaus **300** einen anwendereigenen Bericht oder eine anwendereigene Analyse erstellen, die sie Dritten für eine Gegenleistung bereitstellt. Usage-Clearinghaus **300** kann sich ausbedingen, dass die Personen, denen es den Bericht bereitstellt, diesen Bericht nicht an andere weiterverteilen. Usage-Clearinghaus **300** kann diese Anforderung elektronisch durch Lieferung des Berichts in einem oder mehreren elektronischen Container(n) **152** und durch Aufstellung elektronischer Steuermechanismen **188b** für den Bericht durchsetzen. Diese elektronischen Steuermechanismen **188b** könnten zusammen mit anderen Bedingungen und/oder Beschränkungen (beispielsweise der Bericht darf nicht verändert werden, der Bericht darf ausgedruckt und angesehen werden, es können Auszüge vom Bericht angefertigt werden etc.) der Durchsetzung des „Weiterverteilungs-Verbots" dienen.

[0300] Wie vorstehend erwähnt, kann Usage-Clearinghaus **300** auch Bilanzabschlüsse **240a** und/oder detaillierte Finanzaufzeichnungen **240b** oder andere Finanzinformationen empfangen sowie seine eigenen Bilanzabschlüsse **240c** und/oder detaillierten Finanzaufzeichnungen **240d** generieren. So könnte das Usage-Clearinghaus **300** einen Dienst für Anbieter von Inhalten bereitstellen, in dem Usage-Clearinghaus **300** von den Anbietern von Inhalten Steuermechanismen **188a** ähnlich jenen empfängt, die an Verbraucher **95** geliefert werden. Auf der Grundlage eines Vergleichs dieser Daten könnte Usage-Clearinghaus **300** Schätzungen dahingehend anstellen, welche Geldbeträge die Anbieter von Inhalten von den Finanz-Clearinghäusern **200** erwarten können. Usage-Clearinghaus **300** könnte so eine unabhängige Auditfunktion bereitstellen und damit die Finanz-Clearinghäuser **200** noch ein weiteres Mal überprüfen, womit eine Funktion zur Aufdeckung von Betrug bereitgestellt wird (beispielsweise Personen, die Benutzungsaufzeichnungen vorlegen, zu denen keine Zahlungen stattgefunden haben, oder es können anderweitige falsche Zahlungsbeträge durch Usage-Clearinghaus **300** aufgedeckt werden). Ferner könnte der Steuermechanismus **188** geschlossene Modelle darstellen, die Anbieter von Inhalten zur Implementierung vorgesehen haben, und Usage-Clearinghaus **300** könnte hierzu einen Dienst anbieten, der darin besteht, dass es einen Vergleich mit den tatsächlich gewonnenen Benutzungsdaten zur

modellhaften Darstellung der möglichen finanziellen Ergebnisse, wie sie aussehen könnten, wenn der Anbieter von Inhalten das vorgeschlagene Modell tatsächlich umsetzte, veranstaltet.

[0301] Fig. 34 zeigt eine exemplarische Architektur von Usage-Clearinghaus **300**. In diesem Beispiel enthält Usage-Clearinghaus **300** eine sichere Datenübertragungseinrichtung **346**, eine Datenbank und einen Transaktionsverarbeiter **348**, einen Authentifizierer **350**, einen Berechtigungsprüfer **352** und einen Datenaggregator **354**. Die Architektur von Usage-Clearinghaus **300** kann auf der Architektur des Rechte-Betriebssystems (Rights Operation System) gemäß Fig. 12 und Fig. 13 der Offenbarung des Patents von Ginter et al. basieren.

[0302] Der sichere Datenverkehr **346** stellt in diesem Beispiel einen Datenverkehr mit verschiedenen elektronischen Geräten **100** über ein elektronisches Netzwerk **150** unter Verwendung sicherer Container **152** bereit. Die Datenbank und Transaktionsverarbeiter **348** erfüllen in diesem Beispiel die meisten der in Fig. 33 dargestellten Funktionen. Ein Authentifizierer **350** kann verwendet werden, um Verbraucher und/oder Daten zu authentifizieren, ein Berechtigungsprüfer **352** kann verwendet werden, um Berechtigungen zu überprüfen, und ein Datenaggregator **354** kann verwendet werden, um die Datenaggregationsfunktion **324** auszuführen. Authentifizierer **350** und Berechtigungsprüfer **352** erfüllen Authentifizierungsfunktionen, wie in der Offenbarung von Ginter et al. in Verbindung mit sicheren elektronischen Geräten und geschützten Verarbeitungsumgebungen beschrieben.

[0303] Fig. 35 zeigt ein Beispiel für einen Usage-Clearing-Gesamtablauf. In diesem Beispiel stellt Anbieter **164** den Verbrauchern **95(1)**, **95(2)**, **95(3)** digitale Eigenschaften bereit. Beispielsweise könnte Anbieter **164** in einem elektronischen Container **152** für jeden Verbraucher **95** einen Roman oder ein anderes Werk **166** bereitstellen. Dem Werk **166** kann ein oder mehrere Regelsätze **188** beigeordnet werden (und in einem Beispiel in demselben elektronischen Container **152** zugestellt werden, in dem auch das Werk **166** geliefert wird). Die Steuermechanismen **188** können vorgeben, dass bestimmte Typen Benutzungsdaten in Form einer Prüfkette gewonnen werden müssen, und dass die Prüfkette auf der Grundlage bestimmter zeitbezogener und/oder anderer Ereignisse übergeben werden muss.

[0304] Da Container **152** nur innerhalb einer sicheren geschützten Verarbeitungsumgebung **154** geöffnet werden kann, die Teil der in der oben genannten Offenbarung des Patents von Ginter et al. beschriebenen virtuellen Verteilungsumgebung ist, kann Anbieter **164** sich darauf verlassen, dass die erforderlichen Prüfketten so generiert und gemeldet werden, wie er dies vorgegeben hat. Da Verbraucher **95** die Eigenschaft **166** benutzen, erfassen und speichern deren elektronischen Geräte **100** automatisch die Benutzungsdaten in Form von Prüfketten **302**. Hiernach, beim Eintreten eines vorgegeben Ereignisses (beispielsweise ein Mal im Monat, ein Mal pro Woche, nach einer bestimmten Anzahl Benutzungen etc.) senden die verbraucherseitigen elektronischen Geräte **100** Prüfketteninformationen **302** in einem digitalen Container an Usage-Clearinghaus **300**.

[0305] Usage-Clearinghaus **300** gewinnt die Prüfketteninformationen **302**, speichert diese ggf. in seiner Datenbank **316** und analysiert die Prüfketteninformationen, um einen Bericht **304** zu generieren, den es in einem weiteren elektronischen Container **152** an Anbieter **164** senden kann.

[0306] Anbieter **164** empfängt automatisch sichere Information darüber, wie oft und wie sein Werk benutzt wurde, womit Usage-Clearinghaus **300** den Anbieter von seiner Aufgabe befreit, diese detaillierten Benutzungsdaten selbst zu gewinnen oder zu analysieren. Ferner kann Usage-Clearinghaus **300** dazu eingesetzt werden, die Datenschutzinteressen der Verbraucher **95** durch Offenlegung nur solcher zusammengefasster Daten zu schützen, zu deren Übermittlung es durch die Verbraucher bevollmächtigt wurde (beispielsweise wie viele Verbraucher das Werk **166** benutzt haben, nicht aber die Namen oder Adressen der Verbraucher). Diese Vertraulichkeitsfunktion würde mehr Schwierigkeiten bzw. Probleme bereiten, sollte Anbieter **164** versuchen, die detaillierten Usage Records selbst zu analysieren.

[0307] Fig. 36 zeigt ein detailliertes Beispiel für einen Usage-Clearing-Ablauf unter Beteiligung zweier verschiedener Usage-Clearinghäuser **300(1)**, **300(2)**. In diesem Beispiel liefert Anbieter **164** ein Werk **166** direkt an die Verbraucher **95** sowie an die Händler **168**, die das Werk an die Verbraucher weitervertreiben können. Die den verteilten Inhalten **166** beigeordneten Steuermechanismen **188** können vorgeben, dass das Usage-Clearinghaus **300(1)** Informationen in Bezug auf die Benutzung durch den Ersteller **164** direkt verteilter Inhalte **166** gewinnen und analysieren muss, und dass ein weiteres Usage-Clearinghaus **300(2)** Benutzungsdaten gewinnen und analysieren muss, die sich auf die Benutzung des Werks **166** beziehen, wie es durch den Händler **168** vertrieben wird. Alternativ können Usage-Clearinghäuser **300(1)**, **300(2)** unterschiedliche Benutzungsdaten in Bezug auf dieselbe elektronische Eigenschaft **166** gewinnen (beispielsweise könnte ein Usage-Clearinghaus Informationen in Bezug auf einen Pay-per-View-Gebrauch gewinnen, während das andere Usage-Clearinghaus Benutzungsdaten für alle Einmaleinkäufe gewinnen könnte). Die Usage-Clearinghäuser **300(1)**, **300(2)** können jeweils für den Ersteller **164** und/oder Händler **168** und/oder Verbrau-

cher **95** Berichte **304** ausgeben.

[0308] Fig. 37 zeigt, wie ein Usage-Clearinghaus **300** in Kombination mit einem Finanzclearinghaus **200** eingesetzt werden kann. In diesem Beispiel kann ein verbraucherseitiges elektronisches Gerät **100**

- Prüfketteninformationen **302** in Bezug auf die Benutzung elektronischer Inhalte an Usage-Clearinghaus **300** senden, und
- Prüfketteninformationen **228** über Benutzung und Zahlung in Bezug auf Finanzclearing-Aktivitäten an Finanz-Clearinghaus **200** senden.

[0309] Bei Bedarf können Usage-Clearinghaus **300** und Finanz-Clearinghaus **200** durch dasselbe Geschäft betrieben werden (in diesem Fall könnten sowohl Usage- als auch Finanz-Prüfketteninformationen in ein und demselben elektronischen Container **152** versandt werden). Die von Usage-Clearinghaus **300** ausgeführten Usage-Clearingfunktionen können parallel zu den durch Finanz-Clearinghaus **200** ausgeführten Finanz-Clearingfunktionen betrieben werden, um sowohl ein detailliertes Usage Reporting als auch ein effizientes Finanzclearing zu unterstützen.

[0310] Fig. 38 zeigt ein weiteres Beispiel für einen Usage-Clearingvorgang auf der Grundlage von Content Placement in Medien und/oder in der Werbung. Die Verbraucher **95(1)**, **95(2)**, **95(N)** können verschiedene Informationsverteilungs-Dienste **170A**, **170B**, ... abonnieren. Diese Informationsverteilungs-Dienste **170** können von Anbieter von Inhalten **164** produziertes Sendungsmaterial und Werbeinhalte (kommerzielle Inhalte) vertreiben. Verbraucher **95** konsumieren die verteilten Inhalte, und ihre elektronischen Geräte **100** gewinnen und übergeben die hierzu gehörigen Benutzungsdaten an die Usage-Clearinghäuser **300(1)**, **300(2)**....

[0311] Die Usage-Clearinghäuser **300** können mithilfe der erhaltenen Benutzungsdaten demographische Analysen durchführen und auf Grundlage dieser demographischen Analysen bestimmte Werbung auf andere kommerzielle Inhalte **164** für bestimmte Informationsdienste **170** ausrichten. So könnte etwa Informationsdienst **170A 164** für Läufer und andere Personen mit Interesse an körperlicher Fitness interessantes Sendungsmaterial und kommerzielle Inhalte vertreiben. Usage-Clearinghaus **300(1)** könnte die durch solche Verbraucher **95** bereitgestellten Benutzungsdaten analysieren, die diesen Informationstyp subskribieren und sich ansehen. Usage-Clearinghaus **300(1)** ist damit in der einzigartigen Lage, Werbung in anderen kommerziellen und nichtkommerziellen Inhalten zu platzieren, die für dieselbe Interessengruppe von Interesse sein könnte. In ähnlicher Weise, könnte Informationsdienst **170B** sich auf die Verbreitung von Informationen von Interesse für Autoliebhaber spezialisieren. Usage-Clearinghaus **300(2)** kann Benutzungsdaten über die Benutzung dieses Informationstyps gewinnen und befindet sich damit in einer günstigen Position, die es ihm auf einzigartige Weise erlaubt, Werbeinhalte, kommerzielle und nichtkommerzielle Inhalte an diese Verbrauchergruppe zielgerichtet zu vertreiben.

[0312] Fig. 39 zeigt ein weiteres Beispiel für einen Usage-Clearingvorgang, der durch Usage-Clearinghaus **300** ausgeführt werden kann. In diesem Beispiel kann Usage-Clearinghaus **300** von Rechteinhaber **164** dazu bevollmächtigt werden, Nachlässe auf Grundlage der Menge Benutzungsdaten anzubieten, die ein Verbraucher **95** offen zu legen bereit ist. Dies kann beispielsweise mithilfe der Steuermechanismen **188** für die Eigenschaft durch Auswahl unter Regelsätzen und/oder durch Aufnahme elektronische Verhandlungen (siehe Ginter et al. **Fig.** 76A und B) erfolgen. Rechteinhaber könnten dies als allgemeine Regel für ihre Eigenschaft vorsehen, oder bestimmte Rechte- und Berechtigungs-Clearinghäuser **400** könnten (z. B. auf der Grundlage ihrer speziellen Stellung als Erfasser bestimmter Kategorien von Benutzungsdaten) dazu bevollmächtigt werden, diese Regelsätze zu liefern.

[0313] Beispielsweise könnte das verbraucherseitige elektronische Gerät ein Personalcomputer sein, und Rechteinhaber **164**, die Computersoftware vertreiben, können sich dafür interessieren, welche Programme die Verbraucher **95** zusätzlich zu jenen, die sie selbst vertreiben, verwenden. Andererseits kann Verbraucher **95** eine Offenlegung dieser detaillierten Informationen über die auf seinem Personalcomputer installierten Programme nicht wünschen.

[0314] Als ein weiteres Beispiel kann Rechteinhaber **164** des digitalen Fernsehens alles über alle Fernsehsendungen wissen wollen, die Verbraucher **95** sich ansieht, während der Verbraucher u. U. nicht wünscht, dass andere erfahren, für welche Programme er sich interessiert Usage-Clearinghaus **300** kann diesen entgegengerichteten Interessen effektiv Rechnung tragen, indem dem Verbraucher **95** finanzielle Anreize für mehr vollständige Offenlegung geboten werden, dem Verbraucher dabei jedoch die Wahl gelassen wird.

[0315] In diesem Beispiel vertreibt Rechteinhaber **164** elektronische Inhalte und auf diese angewandte Steuermechanismen an Verbraucher **95**. Die Steuermechanismen können Optionen für die Offenlegung von Benutzungsdaten vorgeben. Der Verbraucher kann zwischen den folgenden Optionen wählen:

- vollen Preis zahlen und sämtliche für die Zahlung nicht erforderlichen Benutzungsdaten absolut geheim halten;
- Gewährung einer beschränkten Offenlegung von Benutzungsdaten gegen kleine Nachlässe; oder
- Inanspruchnahme großer Nachlässe für vollständige Offenlegung der Benutzungsdaten.

[0316] Einige auf den Datenschutz besonders bedachte Verbraucher mögen wollen, dass die Außenwelt so wenig wie möglich über ihr Benutzerverhalten erfährt und dafür bereit sein, den vollen Preis für den Schutz ihrer Privatsphäre zu zahlen. Andere Verbraucher mögen sich keine Gedanken darüber machen, was die Außenwelt über ihr Benutzerverhalten weiß und es dafür auf große Preisnachlässe auf der Grundlage von mehr vollständiger Offenlegung abgesehen haben. Es können beliebig viele solcher Optionsebenen bereitgestellt werden, womit dem Verbraucher beispielsweise die Möglichkeit gegeben wird, präzise auszuwählen, welche Arten von Informationen offen gelegt, und welche geheim gehalten werden. Da die Benutzungsdaten innerhalb einer sicheren geschützten Verarbeitungsumgebung **154** gewonnen werden, die Teil des verbraucherseitigen elektronischen Geräts **100** ist, können sich die Verbraucher darauf verlassen, dass die Benutzungsdaten sicher übergeben werden, und dass eine unerlaubte Offenlegung ohne seine Zustimmung nicht stattfinden wird.

[0317] Auf Grundlage beispielsweise eines oder mehrerer jener Regelsätze **188**, die der geschützten Verarbeitungsumgebung **154** des Verbrauchers bereitgestellt werden, und/oder auf Grundlage der durch solche Regelsätze bereitgestellten Wahlmöglichkeit des Verbrauchers könnte die geschützte Verarbeitungsumgebung **154** des Verbrauchers gegenüber Usage-Clearinghaus **300** keine (oder minimale) Benutzungsdaten, ausgewählte Benutzungsdaten oder sämtliche Benutzungsdaten offen legen. Usage-Clearinghaus **300** kann hiernach ungehindert die von ihm gewonnenen beschränkten und vollständigen Benutzungsdaten analysieren und dadurch den Rechteinhabern **164** und anderen Dritten wie Marktforschern, Brokern, Werbetreibenden, Auditoren, Wissenschaftlern und anderen Berichte und Analysen bereitstellen.

Rechte- und Berechtigungs-Clearinghaus

[0318] Fig. 40 zeigt ein Beispiel für ein Commerce Utility System **400** vom Typ Rechte- und Berechtigungs-Clearinghaus. Die Dienste von Rechte- und Berechtigungs-Clearinghäusern können eine beliebige Kombination aus den folgenden Gesamtfunktionen ausführen:

- Registrierung digitaler Objekte und hierzu gehöriger Berechtigungen, Preise und/oder anderer genehmigter und/oder erforderlicher Vorgänge, die die Ausführung von Konsequenzen für die Durchführung und/oder Nichtdurchführung solcher Vorgänge unterstützen;
- Bereitstellung vorab bestätigter Berechtigungen auf Verlangen gemäß vorgegebenen Umständen und/oder anderen Anforderungen wie Klassen von Anforderern von Berechtigungen, die Erfüllung oder die Fähigkeit, Zahlungsanforderungen zu erfüllen etc.;
- Sichere und effiziente elektronische Copyright-Anmeldung bei der betreffenden Stelle für ein oder mehrere Länder und/oder andere unter eine bestimmte Gerichtsbarkeit fallende Einheiten; und
- Berichterstattungsfunktionen.

[0319] Genauer unterstützen Rechte und Berechtigungen Dienste in Übereinstimmung mit diesen Erfindungen, die beispielsweise einige oder alle der folgenden Funktionen und Merkmale umfassen können:

- Identifikation, Verteilung und Verifikation bestimmter Eigentumsrechte und/oder anderer geschäftsbezogener Regeln und Steuermechanismen über eine digitale elektronische Wertkette.
- Bereitstellung von Objekt-Registry-Diensten und Rechten, Preisen und/oder anderen Kontrollinformationen für registrierte Objekte.
- Zuweisung für jedes digitale Objekt mindestens einer Identifikationsnummer und/oder eines Namens in Übereinstimmung mit seinem eigenen Nummerierungs- und/oder Benennungssystem und/oder in Übereinstimmung mit einem oder mehreren Nummerierungs- und/oder Benennungssystemen einer oder mehrerer anderer Organisationen, Gesellschaften (beispielsweise Standardorganisationen), Firmen und/oder Geschäftsstellen (beispielsweise staatliche Kontrollbehörden).
- Empfang einer Vollmacht von der sicheren Kette der Verarbeitung und Steuerung in Form elektronischer Regelsätze.
- Sichere Bereitstellung von Berechtigungen (beispielsweise Beschreibungen genehmigter Vorgänge und hiermit verbundener Konsequenzen wie Preise auf der Grundlage von Regeln und Steuermechanismen) für digitale Eigenschaften, die registriert wurden, und Unterstützung der automatisierten Verknüpfung solcher registrierter Eigenschaften mit Sätzen von Regeln und Steuermechanismen (beispielsweise Aktualisierung der Regeln und Steuermechanismen, Einsatz voreingestellter Templates auf der Grundlage von Eigenschaftsklassen etc.), die beispielsweise zumindest teilweise von einem fernen Gerät bereitgestellt und während oder infolge einer solchen Registrierung sicher zum registrierenden Standort gedownloadet werden können.
- Ausstattung von Rechteinhabern an digitalen Inhalten mit der Möglichkeit, für ein oder mehrere Rechte- und Berechtigungs-Clearinghäuser Modi zu bestimmen und flexibel zu definieren und sicher bereitzustellen, in denen sie Produkte ihres geistigen Eigentums (beispielsweise VDE-geschützte digitale Eigenschaften) benutzt oder nicht benutzt sehen wollen, sowie Konsequenzen eines solchen Gebrauchs und/oder Missbrauchs festzulegen.

• Bereitstellung VDE-gestützter Möglichkeiten der Verteilung und Verwaltung von Rechten und Geschäftsregeln (einschließlich vorab bestätigter und andere Berechtigungen) in einer elektronischen ad-hoc-Wertkette, wobei solche Rechte und Geschäftsregeln dauerhaft unterstützt werden.
• Bereitstellung von Berechtigungen für digitale Objekte auf Verlangen für Personen, die zur Benutzung eines digitalen Objekts befugt sind.
• Kann auf der Grundlage verschiedener, mit einer oder mehreren Benutzerklassen-Kombinationen (beispielsweise unterschiedliche Altersgruppen, Gerichtsbarkeiten, geschäftliche Möglichkeiten, Verbraucher, Ersteller, Anbieter, Partner, Regierung, gemeinnützige Organisationen, Bildungsstätten, Mitgliedschaft in Organisationen etc.) sicher beigeordneter Berechtigungen unterschiedliche Bedingungen bereitstellen.
• Zusicherung gegenüber Rechteinhabern, dass die von ihnen festgelegten Bedingungen durch eine potentielle vielförmige und verteilte Wertketten-Teilnehmerbasis eingehalten werden.
• Kann Steuermechanismen bereitstellen, die nicht alle möglichen Berechtigungen umfassen und/oder weitere, erforderliche und/oder gewünschte Berechtigungen auf Verlangen ad-hoc und/oder vorgeplant gemäß den Rechten des Anforderers (Klasse und/oder einzelner) vertreiben, wodurch sich Rechteinhaber beispielsweise dazu entscheiden können, nur die am häufigsten benutzten, einer bestimmten digitalen Eigenschaft beigeordneten Berechtigungen zu vertreiben, wodurch die betreffenden Parteien in die Lage versetzt sind, in Übereinstimmung mit dem Modell des Rechteinhabers neue Berechtigungen zu erwerben.
• Erneuerung ausgelaufener Berechtigungen auf Verlangen und/oder bei automatisierter Erkennung des Auslaufens solcher Rechte unter Verwendung von Clearinghaus-Datenbankmechanismen und mittels automatisierter Bereitstellung und/oder Aufforderung zur Bereitstellung solcher Berechtigungen und/oder in der bevorzugten Ausführungsform Unterrichtung eines VDE-Wertketten-Teilnehmers von der Notwendigkeit des Erwerbs solcher Berechtigungen (den betreffenden Benutzer beispielsweise unterrichten, bevor der Benutzer aktiv versucht, entsprechende Informationen und/oder elektronische Steuerabläufe zu benutzen, womit eine Frustration des Benutzers und Ineffizienz vermieden werden).
• Einsatz sicherer Container wie die in Ginter et al. beschriebenen in jedem Schritt, Teil oder Vorgang bei der Bereitstellung sicherer Rechteclearingdienste.
• Erstellung, Speicherung, Verteilung, und Empfang von Rechte- und Berechtigungs-„Templates", mit denen Rechteinhaber effizient und adäquat Rechte, Bedingungen und Konsequenzen (beispielsweise Entschädigung) vorgeben können, die Vorgängen der Benutzung ihrer digitalen Eigenschaften (und/oder der Benutzung durch VDE-Vorgänge gesteuerter elektronischer Ereignisse) beigeordnet werden.
• Templates können direkt mit digitalen Regelsätzen korrespondieren, die Eigenschaften, Benutzern von Inhalten, Benutzerklassen und/oder anderen digitalen Informationen und/oder physischen oder virtuellen Standorten und/oder Prozesssteuerung für die Kontrolle über Ereignisse und Ereignis-Konsequenzen zugeordnet sind.
• Templates können selbstausführend sein.
• Templates können auf mehrere Objekte/Fälle anwendbar sein.
• Templates können unabhängig von digitalen Objekten geliefert werden, denen sie möglicherweise beigeordnet sind.
• Templates sind erweiterbar und offen für neue Vorgänge und Szenarien einschließlich aber nicht beschränkt auf neue Zahlungsmethoden, Preismodelle und Preisebenen sowie neue Berechtigungen.
• Templates können alle möglichen digitalen Rechte wie beispielsweise Verteilungs- und Übermittlungsrechte und/oder Rechte für eine wiederholte Übermittlung flexibel erkennen.
• Templates können individuelle Identitätsrechte und/oder Klassenidentitätsrechte flexibel erkennen.
• Unterschiedliche Templates können auf unterschiedliche Typen von Anordnungseigenschaften der Inhalts- und/oder Prozesssteuerung anwendbar sein.
• Es können mehrere Templates auf dieselbe Anordnung von Eigenschaften und/oder Prozesssteuerung anwendbar sein.
• Ein Rechte- und Berechtigungs-Clearinghaus/Rechte- und Berechtigungs-Clearinghäuser kann (können) Templates von übergeordneten Sätzen (Superset Templates) führen, mit deren Hilfe Teilnehmer der Wertkette und/oder hierarchisch untergeordnete Clearinghäuser ein oder mehrere solcher Superset Templates modifizieren können, um Templates zu erstellen, die einen Teilsatz und/oder erweiterten Satz dieses einen bzw. dieser mehrerer Superset Templates einsetzen.
• Templates können auf verschiedene Art und Weise hergestellt werden, beispielsweise unter Verwendung einer graphischen Benutzeroberfläche und/oder einer Rechteverwaltungs-Sprache.
• Es können Template-„Anwendungen" unter Einsatz einer topographischen, schematischen, direkt editierbaren graphischen Darstellung von Wertketten-Regeln und -Steuermechanismen erstellt und/oder verändert werden, wobei solche Regeln und Steuermechanismen und Wertkettenbeziehungen über das Display mit Informationen beispielsweise in einer Mischung aus Icons, Positionsinformationen, Flussdiagrammen und Textin-

formationen dargestellt werden, und wobei die Regeln und Steuermechanismen beispielsweise unter Verwendung einer Rechteverwaltungssprache implementiert sind, wobei beispielsweise Elemente oder die Darstellung solcher Elemente der Rechtesprache auf höherer Ebene direkt mit graphischen Darstellungskomponenten korrespondieren kann.

• Es können mehrere Teilnehmer der Wertkette an der Erstellung von Templates mitwirken und/oder diese verändern und/oder an der Erstellung verschiedener, auf dieselben digitalen Informationen angewandter Templates mitwirken und/oder diese verändern.

• Benutzer können zwischen unterschiedlichen Templates wählen, die auf dieselben digitalen Informationen anwendbar sind, einschließlich beispielsweise digitaler Informationen, die Steuerungsabläufe (z. B. Informationen zum Ereignismanagement) beschreiben und/oder regeln, die beispielsweise über eine sichere VDE-Kette der Verarbeitung und Steuerung verwaltet werden.

• Die Verteilung von Rechte-Clearingfunktionen in einem Netzwerk oder einem anderen System (beispielsweise ist jeder Verbraucher und/oder anderer Wertkette-Teilnehmer-Knoten potentiell ein verteilter Rechteclearingdienst, der mindestens teilweise sein eigenes sicheres Rechteclearing auslöst, wobei dieser Teilnehmerknoten Rechteinformationen direkt an einen oder mehrere andere Teilnehmer, interoperable Clearing-Knoten übermitteln kann, in der bevorzugten Ausführungsform verwenden alle Aktivitäten VDE-Techniken wie jeweils anwendbar und wie in der Patentschrift Ginter, et al. beschrieben).

• Erteilung einer Vollmacht und/oder Bereitstellung von Diensten für oder in Verbindung mit, ein(em) oder mehrere(n) untergeordnete(n) Rechte-Clearinghäuser(n), deren Vorgänge von einem anderen Ort logisch und/oder physisch lokalisiert werden können, wie etwa innerhalb eines Unternehmens oder einer Behörde und/oder innerhalb einer oder mehrerer Gerichtsbarkeit(en) und/oder im Dienst von Teilmengen des Gesamtgeschäfts eines übergeordneten Rechte-Clearinghauses, welches Rechte-Clearingfunktionen in einem System oder Netzwerk verteilt und/oder anderweitig autorisiert, beispielsweise wo jeder Verbraucher und/oder ein bestimmter oder alle anderen Wertkettenteilnehmer-Knoten potentiell einen verteilten Usage-Clearing-Dienst unterstützen können, der seine eigenen sicheren Rechteclearing-Transaktionen und -Funktionen in der Umgebung des Clearinghaus-Gesamtnetzwerks auslöst einschließlich der Clearinghaus-Interoperation mit interoperablen Knoten eines oder mehrerer anderer Teilnehmer und, wie auch an anderer Stelle in dieser Liste, sämtlicher Aktivitäten, die beispielsweise VDE-Techniken wie jeweils anwendbar einsetzen.

• Eines oder mehrere Recht(e) kann (können) einem Teilnehmer zumindest teilweise auf Grundlage einiger Aspekte der Benutzung von Inhalts- und/oder Prozesssteuerung automatisch bereitgestellt werden, und ein oder mehrere dergestalt bereitgestellte(s) Recht(e) kann (können) beispielsweise als eine Promotions-Komponente geliefert werden, bei der Gutscheine als Gegenleistung für bestimmte Benutzungs- (beispielsweise Einkaufs-) Profile bereitgestellt werden, die direkt aus Benutzungsdaten gewonnen oder aus einer gewichteten Formel unter Beteiligung mehrerer Variablen ermittelt werden können.

• Kann hierarchisch, nach dem Peer-to-Peer-Prinzip oder in einer kombinierten Form organisiert sein wobei die Verantwortung für das Rechteclearing für verschiedene Handelsmodelle und/oder Aktivitäten und/oder Wertketten auf verschiedene Weise verteilt sein kann, wobei eine bestimmte oder mehrere Parteien beispielsweise in einem Fall oder mehreren Fällen hierarchisch anderen Parteien übergeordnet, in einem anderen Fall oder mehreren anderen Fällen jedoch hierarchisch ein Peer oder untergeordnet sein kann (können), d. h. die Beziehung zwischen Teilnehmern ist programmierbar und kann dergestalt eingerichtet (und nachträglich verändert) werden, dass für bestimmte gewerbliche Tätigkeiten, Wertketten oder Modelle eine oder mehrere gewünschte Rechteclearing-Konfiguration(en) entstehen.

[0320] Fig. 40 zeigt ein Beispiel für ein Rechte- und Berechtigungs-Clearinghaus **400** aus funktioneller Sicht. In diesem Beispiel kann Rechte- und Berechtigungs-Clearinghaus **400** einige oder alle der folgenden vier Hauptfunktionen ausführen:

• Objektregistrierung. Das Rechte- und Berechtigungs-Clearinghaus **400** registriert digitale Eigenschaften und die ihnen beigeordneten Berechtigungen und Preise.

• Berechtigungen auf Verlangen. Auf Anfrage stellt Rechte- und Berechtigungs-Clearinghaus **400** Berechtigungen **188** zusammen mit den ihnen beigeordneten Preisen in sicheren elektronischen Containern **152** bereit. Die Steuermechanismen **188** für Berechtigungen können unabhängig von den Inhalten bereitgestellt werden.

• Ausgehandelte Berechtigungen. Bei Erhalt entsprechender Anfragen und Aufforderungen verhandelt das Rechte- und Berechtigungs-Clearinghaus **400** Berechtigungen und/oder Preise im Namen von Rechteinhabern aus, die diese Verantwortung dem Rechte- und Berechtigungs-Clearinghaus übertragen haben. Das Rechte- und Berechtigungs-Clearinghaus **400** kann auch bei Verhandlungen zwischen dem Rechteinhaber und dem Rechtebenutzer vermitteln. Rechteinhaber und Rechtebenutzer können untereinander verhandeln und das ausgehandelte Ergebnis an das

Rechte- und Berechtigungs-Clearinghaus melden.

• Berichterstattung. Rechte- und Berechtigungs-Clearinghaus **400** kann Berichte bereitstellen, um die Berichterstattung seitens der Finanz-Clearinghäuser **200** und/oder Usage-Clearinghäuser **300** zu verbessern.

[0321] In diesem Beispiel kann Rechte- und Berechtigungs-Clearinghaus **400** einige oder alle der folgenden Funktionen bereitstellen:

• Erstellung, Aktualisierung oder Abänderung **408** von Berechtigungen,
• Berechtigungsverteilung **410**,
• Datenbankverwaltung **412**,
• Templatedefinitionen und/oder -verwaltung **414**,
• Aushandlung von Berechtigungen **416**,
• Berichterstattung **417**,
• Replikation **418**,
• Propagierung **420**.

[0322] Die dem Rechte- und Berechtigungs-Clearinghaus **400** zufallende Primäraufgabe der Objektregistrierung wird durch Datenbankverwaltung **412** ausgeführt. In Verbindung hiermit kann Rechte- und Berechtigungs-Clearinghaus **400** Regelsätze **188** und entsprechende Objektidentifikationen **422** in ein und demselben elektronischen Container **152** oder in verschiedenen elektronischen Containern **152** empfangen und diese Informationen hiernach in einer Datenbank **412** „registrieren", um später darauf verweisen zu können. Rechte- und Berechtigungs-Clearinghaus **400** kann Rechteinhaber durch Bereitstellung einer Templatefunktion **414** bei der Definition von Regelsätzen **188** unterstützen, mit denen Rechte und Berechtigungen in Bezug auf elektronische Eigenschaften des Rechteinhabers festgelegt werden. Zusätzlich zu Objekten oder Eigenschaften **166** können der Registrierungsvorgang **419** und die Datenbank **412** auch Regelsätze **188** registrieren.

[0323] Die Datenbankfunktion **412** und die Verteilungsfunktion **410** von Rechte- und Berechtigungs-Clearinghaus **400** kann zur Verteilung von Berechtigungen nach Eingang der Anforderungen **402** verwendet werden und kann ferner dafür verantwortlich sein, (über Verteilungsfunktion **410**) sämtliche Berechtigungen in Bezug auf eine bestimmte Eigenschaft zu vertreiben. Da Berechtigungen und/oder Preise auslaufen bzw. sich ändern können, kann das Rechte- und Berechtigungs-Clearinghaus **400** auch dafür verantwortlich sein, Regelsätze **188** zu aktualisieren, die bereits ausgegebene Berechtigungen und/oder Preise festlegen, sowie solche aktualisierten Regelsätze zu vertreiben.

[0324] Rechte- und Berechtigungs-Clearinghaus **400** kann auch eine Berichterstattungsfunktion **417** bereitstellen, beispielsweise zur Erstellung von Berichten **406** in Bezug auf die erteilten oder vertriebenen Berechtigungen und/oder Preise. In diesem Beispiel stellt der Betrieb von Rechte- und Berechtigungs-Clearinghaus **400** Auditmöglichkeiten bereit, i. e. einen Kanal, über den Benutzungsdaten angefügt werden. Solche Audit-Vorgänge (die beispielsweise dadurch bereitgestellt werden können, dass Funktionen des Rechte- und Berechtigungs-Clearinghauses **400** in Funktionen des Usage-Clearinghauses **300** integriert werden) könnten dazu verwendet werden, integrierte Berichte darüber zu auszustellen, welche Berechtigungen bereitgestellt, und welche Berechtigungen ausgeübt wurden – sehr wertvolle Informationen für die Marktforschung und für Auswirkungen auf das Geschäft, womit eine verbesserte Nachvollziehbarkeit für den Rechteinhaber bereitgestellt wird.

[0325] Diese Auditfunktion von Rechte- und Berechtigungs-Clearinghaus **400** kann sich als besonders vorteilhaft erweisen, wenn es um die Wahrung der Vertraulichkeit geht. So könnte etwa ein privates Rechte- und Berechtigungs-Clearinghaus **400** dergestalt erweitert werden, dass es eine Zahlungsaggregation bereitstellt, um vertrauliche Informationen auf der Ebene individueller Transaktionen vor einem Zugriff des Finanz-Clearinghauses **200** zu schützen. In einem weiteren Beispiel kann ein Rechte- und Berechtigungs-Clearinghaus **400** Berichte **426** ausstellen, in denen beispielsweise die Anzahl der zu Beginn einer Berichterstattungsperiode in der Datenbank **412** registrierten Objekte, die Anzahl neuer registrierter Objekte sowie verschiedene aggregierte statistische Daten enthalten sind, etwa in Bezug auf die Anzahl Arten der diesen Objekten beigeordneten Berechtigungen und/oder Durchschnitts- oder Zentralwerte für Preise für bestimmte Objektarten.

[0326] Rechte- und Berechtigungs-Clearinghaus **400** kann auch Anforderungen **402** mit Antworten **428** beantworten. Eine Anforderung kann beispielsweise in einer automatisch erteilbaren Anforderung von Berechtigungen bestehen; oder die Anforderung erfordert möglicherweise einen Berechtigungsnachweis seitens des Rechte- und Berechtigungs-Clearinghauses **400**, damit festgestellt werden kann, ob der Anfordernde die Berechtigungen empfangen darf. Ein Anspruch könnte durch Vorlage eines oder mehrerer gültiger Zertifikate festgestellt werden, die einfach in der Datenbank **412** zur Übertragung an Anbieter zusammen mit anderen Informationen über durch das Clearinghaus erteilte Berechtigungen überprüft oder gespeichert werden könnten. In der bevorzugten Ausführungsform könnte ein anderer Anspruch auf einem gemeinsamen Geheimnis basieren (beispielsweise ein oder mehrere Tag(s) eines vom Anfordernden geführten Regelsatzes **188**), das die PPE **54** des Anfordernden und das Rechte- und Berechtigungs-Clearinghaus **400** kennen. Dieses gemeinsame Geheimnis könnte in Kombination mit einem Zertifikat verwendet werden oder – in Fällen, wo die Anforderungen an einen Anspruch niedriger sind oder

bereits festgestellt wurden (beispielsweise indem das gemeinsame Geheimnis zuerst erhalten wurde) – das gemeinsame Geheimnis könnte alleine ausreichen, um beispielsweise eine Berechtigung zu empfangen, die eine ausgelaufene Berechtigung ersetzt oder aktualisiert.

[0327] Rechte- und Berechtigungs-Clearinghaus **400** beinhaltet auch eine Permission Negotiation Engine **416**, die zur Aushandlung solcher Berechtigungen **188** eingesetzt werden kann, die nicht vom Rechteinhaber vorab bestätigt wurden. Angenommen ein Verbraucher **95** möchte beispielsweise ein Recht ausüben, das nicht in der Datenbank **412** hinterlegt ist. Der Verbraucher **95** könnte das Recht anfordern. Bei Eintreffen der Anforderung könnte Rechte- und Berechtigungs-Clearinghaus **400** feststellen, ob es vom Rechteinhaber autorisiert ist, im Namen des Rechteinhabers über das Recht zu verhandeln. Hat der Rechteinhaber das Rechte- und Berechtigungs-Clearinghaus **400** nicht zum Verhandeln bevollmächtigt, so könnte das Clearinghaus den Rechteinhaber kontaktieren und eine Vollmacht und/oder die Berechtigung selbst anfordern. Hat der Rechteinhaber das Rechte- und Berechtigungs-Clearinghaus **400** mit einer Verhandlungsvollmacht ausgestattet, so könnte das Clearinghaus in eine elektronische Verhandlung (siehe Ginter et al., **Fig.** 75A-76B) zwischen dem Regelsatz des Verbrauchers und dem Regelsatz des Rechteinhabers eintreten. Der hierbei ausgehandelte Regelsatz könnte dem Verbraucher zugesandt werden, wodurch der Verbraucher das Recht ausüben kann.

[0328] Fig. 41 zeigt eine exemplarische Architektur für das Rechte- und Berechtigungs-Clearinghaus **400**. In diesem Beispiel umfasst das Rechte- und Berechtigungs-Clearinghaus **400** eine sichere Datenübertragungseinrichtung **430**, eine Datenbank und einen Transaktionsverarbeiter **432**, einen Authentifizierer **434**, einen Berechtigungsprüfer **436** und einen Registrierungsverarbeiter **438**. Wie vorstehend besprochen, kann die Architektur von Rechte- und Berechtigungs-Clearinghaus **400** auf der Architektur des Rechte-Betriebssystems gemäß Fig. 12 und Fig. 13 der Offenbarung des Patents von Ginter et al. sowie gemäß dem zugehörigen Text basieren.

[0329] Datenbank und Transaktionsverarbeiter **432** führen die meisten Funktionen gemäß Fig. 40 aus. Der Registrierungsverarbeiter **438** kann die Registrierungsfunktion **419** ausführen. Die Datenübertragungseinrichtung **430** kommuniziert sicher über das elektronische Netzwerk **150** mit den Verbrauchern **95**, den Autoren **164**, den Herausgebern **168**, den Aggregatoren **170**, den Repackagern **174** und anderen Teilnehmern der Wertkette über sichere Container **152**. Authentifizierer **434** und Berechtigungsprüfer **436** führen Authentifizierungsfunktionen aus wie in der Offenbarung des Patents von Ginter et al. in Verbindung mit sicheren elektronischen Geräten und geschützten Verarbeitungsumgebungen beschrieben.

[0330] Fig. 42 zeigt ein Beispiel für einen Rechte- und Berechtigungs-Clearingablauf. In diesem Beispiel versendet Autor **164** an Herausgeber **168** ein Werk **166** zusammen mit einem Regelsatz **188A** einschließlich Steuermechanismus A. In Übereinstimmung mit einer sicheren Kette der Verarbeitung und Steuerung fügt Herausgeber **168** Steuermechanismus B zum Regelsatz hinzu, um einen neuen Regelsatz **188AB** zu erhalten. Herausgeber **168** veröffentlicht das Werk **166** mit Regelsatz **188AB** an die Verbraucher **95**. Herausgeber **168** kann auch einen seltener verwendeten, manchmal dennoch nötigen zusätzlichen Berechtigungssatz C innerhalb eines umfangreicheren Regelsatzes **188ABC** vorgeben (beispielsweise kann Steuermechanismus C Journalisten mit der Möglichkeit ausstatten, bestimmte Teile eines Werks **166** für bestimmte Zwecke zu exzerpieren).

[0331] Herausgeber **168** kann Regelsatz **188ABC** (und bei Bedarf auch Regelsatz **188AB** und Regelsatz **188A**) beim Rechte- und Berechtigungs-Clearinghaus **400** registrieren. Der Herausgeber **168** kann auch zusätzliche "Steuermechanismen für Steuermechanismen", oder "Berechtigungen für Berechtigungen" "D" (beispielsweise Steuermechanismus für die Verteilung wie in Verbindung mit den **Fig.** 79-85 der Offenbarung des Patents von Ginter et al. beschrieben) zusammen mit dem Steuermechanismus **188ABC** einsetzen. Dieser zusätzliche Steuermechanismus "D" kann vorgeben, unter welchen Umständen Rechte A, B und/oder C erteilt werden können (Qualifikation von Credentials, Häufigkeit der Neuausstellung, Anzahl der Steuermechanismen für einen bestimmten Benutzer etc.).

[0332] Der Verbraucher **95** (oder ein beliebiger anderer Anbieter wie ein Aggregator, Repackager, Autor oder weiterer Herausgeber) kann die Kopie eines beliebigen dieser verschiedenen, im Rechte- und Berechtigungs-Clearinghaus **400** registrierten Regelsätze anfordern. Wenn beispielsweise die Verbraucherin **95** eine Journalistin ist, die das Werk **166** in Übereinstimmung mit Regelsatz **188AB** benutzt und das Werk für bestimmte Zwecke zu exzerpieren wünscht, kann sie den übergeordneten Regelsatz **188ABC** anfordern, das Herausgeber **168** zuvor im Rechte- und Berechtigungs-Clearinghaus **400** registriert hat. In einem weiteren Beispiel kann es sein, dass ein Verbraucher **95** in Deutschland den zur Verteilung in den Vereinigten Staaten vorgesehenen Regelsatz **188** erhalten hat und einen Regelsatz anfordern muss, der dem rechtlichen und monetären Umfeld in Europa Rechnung trägt. Zusätzlich kann ein Rechteinhaber zuvor vertriebene Steuermechanismen nachträglich verändern, um neue Rechte hinzuzufügen, einen

„Verkauf" bereitzustellen, Rechte einzuziehen etc., wobei das Rechte- und Berechtigungs-Clearinghaus **400** für die Verteilung dieser neuen Regelsätze auf Verlangen verantwortlich ist.

[0333] Fig. 42A zeigt ein weiteres Beispiel, in dem Verbraucher **95** beim Rechte- und Berechtigungs-Clearinghaus **400** einen Regelsatz **188X** registrieren kann, der zu einem Objekt wie einer Datei oder einem Computerprogramm gehört, das von Verbraucher **95** bereits erhalten wurde. Dieser neue Regelsatz **188X** fordert beim Rechte- und Berechtigungs-Clearinghaus **400** für Verbraucher **95** für das genannte Objekt einen neuen Regelsatz **188Y** an, sobald der beim Rechte- und Berechtigungs-Clearinghaus **400** für dieses Objekt registrierte Steuermechanismus verändert wurde. Das Rechte- und Berechtigungs-Clearinghaus **400** kann den aktualisierten Regelsatz **188Y** automatisch an alle registrierten Benutzer einer bestimmten digitalen Eigenschaft versenden.

[0334] In einem weiteren Beispiel könnte Herausgeber **168** das Werk **166** mit einem sehr eingeschränkten Regelsatz **188X** vertreiben, mit dem Verbraucher **95** nur eine Zusammenfassung betrachten kann, und der das Rechte- und Berechtigungs-Clearinghaus **400** als Anlaufstelle für den Erwerb einer Berechtigung festlegt, die gesamten Inhalte zu benutzen. Verbraucher **95** könnte hiernach Rechte- und Berechtigungs-Clearinghaus **400** kontaktieren, um einen erweiterten Regelsatz **188Y** zu erwerben, der zusätzlich Ebenen der Benutzung ermöglicht. Hierdurch werden ein hohes Maß an Nachvollziehbarkeit und erweiterte Auditing-Möglichkeiten bereitgestellt, da Verbraucher **95** Rechte- und Berechtigungs-Clearinghaus **400** kontaktieren muss, wenn eine zuvor vertriebene Eigenschaft auch wirklich benutzen will. In ähnlicher Weise kann Rechte- und Berechtigungs-Clearinghaus **400** aktualisierte Regelsätze **188Y** bereitstellen, um veraltete zu ersetzen. Dieser Mechanismus könnte beispielsweise dazu benutzt werden, einen über einen Zeitraum variablen Preisnachlass für einen bestimmten Posten bereitzustellen (beispielsweise einen Filmhändler mit der Möglichkeit ausstatten, für einen neu auf dem Markt angebotenen Film sechs Monate nach dessen erstmaliger Erscheinung einen Nachlass anzubieten, ohne schon bei der erstmaligen Erscheinung entscheiden zu müssen, wie groß der Nachlass ausfallen soll).

[0335] Fig. 43 zeigt einen weiteren exemplarischen, durch das Rechte- und Berechtigungs-Clearinghaus **400** ausgeführten Rechte- und Berechtigungs-Clearingvorgang. In diesem Beispiel von Fig. 43 registrieren jeweils die Autoren **164**, die Herausgeber **168**, die Aggregatoren **170** und optional andere zusätzliche Teilnehmer der Wertkette ihre eigenen Regelsätze **188A**, **188B**, **188C** in einem Rechte- und Berechtigungs-Clearinghaus **400**, womit sie potentiell darüber hinaus auch solche Steuermechanismen registrieren, welche den Vertrieb der Steuermechanismen ihrer Anbieter steuern. Rechte- und Berechtigungs-Clearinghaus **400** kann danach einen neuen kombinierten Regelsatz **188ABC** vertreiben, der mit den jeweiligen individuellen Regelsätzen **188A**, **188B**, **188C** konsistent ist, wodurch die jeweiligen Teilnehmer der Wertkette nicht mehr andere Regelsätze formulieren müssen als jenen, um den es ihnen geht. In diesem Beispiel kann Rechte- und Berechtigungs-Clearinghaus **400** auch über eine Schnittstelle mit anderen Organisationen (beispielsweise mit einer Behörde **440** wie dem Copyright Office oder einer anderen Organisation wie einem Berufsverband) verfügen. Rechte- und Berechtigungs-Clearinghaus **400** kann ein Urheberrecht an im Rechte- und Berechtigungs-Clearinghaus **400** registrierten Werken und anderen Objekten automatisch anmelden, womit dem Rechteinhaber solche lästigen Vorgänge leichter gemacht oder abgenommen werden. Bei der für die Anmeldung von Urheberrechten nötigen Interaktion zwischen dem Rechte- und Berechtigungs-Clearinghaus **400** und der Behörde **440** können beispielsweise VDE und sichere Container **152** zum Einsatz kommen.

[0336] Fig. 44A-Fig. 44E zeigen einen zusätzlichen Rechte- und Berechtigungs-Clearingablauf, der mithilfe des Rechte- und Berechtigungs-Clearinghauses **400** ausgeführt werden kann. In diesem Beispiel kann ein Herausgeber **168** eine Eigenschaft **166** und den beigeordneten Regelsatz **188a** für Verbraucher **95** (siehe Fig. 44A) bereitstellen. Die Verbraucherin mag ihr elektronisches Gerät **100** und die hierzu gehörige geschützte Verarbeitungsumgebung **154** dazu benutzen, um einen Zugriff auf Eigenschaft **166** zu versuchen, die Regelsatz **188a** verwendet, dabei jedoch feststellen, dass sie für den Zugriff auf die gewünschte Eigenschaft einen zusätzlichen Regelsatz **188b** benötigt. Das verbraucherseitige elektronische Gerät **100** kann an ein Rechte- und Berechtigungs-Clearinghaus **400** (siehe Fig. 44B) eine Anforderung **402** generieren. Hierauf kann das Rechte- und Berechtigungs-Clearinghaus **400** den durch Verbraucher **95** angeforderten Steuermechanismus **188b** mit den Berechtigungen und der Preisinformation (siehe Fig. 44C) vertreiben. Der Verbraucher kann daraufhin die Eigenschaft **166** in Übereinstimmung mit Regelsatz **188** benutzen und auf Grundlage der Benutzung durch den Verbraucher Benutzungs-/Prüfketteninformationen **302** generieren (siehe Fig. 44D). Das verbraucherseitige elektronische Gerät **100** kann diese Benutzungsdaten an Usage-Clearinghaus **300** melden und die intern gespeicherten Benutzungsdaten löschen und/oder als „ausstehend" freigeben, sobald es vom betreffenden Clearinghaus ein Freigabesignal erhält (siehe Fig. 44E).

Rechtetemplates

[0337] Fig. 45A und Fig. 45B zeigen exemplarische Rechtetemplates **450**, und Fig. 45C zeigt ein Beispiel für einen entsprechenden Regelsatz **188**. Rechtetemplate **450** kann beim „Ausfüllen der leeren" Formen in gewisser Hinsicht analog sein. Rechteinhaber können Rechtetemplates **450** benutzen, um effizient und effektiv die einer bestimmten digitalen Eigenschaft zugeordneten Rechte zu definieren. Solche Templates **450** sind beim Abstecken der allgemeinen Möglichkeiten der Technologie der virtuellen Verteilungsumgebung wie beschrieben in der Offenbarung der Patentschrift von Ginter et al. nützlich, und dies dergestalt, dass die Templates für eine konkrete Inhaltsindustrie, Anbieter, einen Inhaltstypen oder ähnliches offen ist. Hierdurch kann ein Benutzer wie etwa ein Anbieter mit einem für einen konkreten Zweck anwendbaren oder nützlichen fokussierten Menü an Ressourcen vorgestellt werden.

[0338] So können Templates **450** einige Annahmen über Merkmale der Inhalte anstellen oder über andere gesteuerte Informationen, darüber, wie sie aufgeteilt oder anderweitig organisiert werden und/oder über die Attribute, die solche organisatorischen Einheiten haben. Templates **450** vereinfachen den Vorgang der Definition von Berechtigungen und sorgen dafür, dass weniger oder gar kein Spezialwissen und zeitlicher Aufwand nötig ist, um die zugrunde liegenden Möglichkeiten der virtuellen Verteilungsumgebung nutzen zu können. In diesem Beispiel hat der Benutzer gegebenenfalls die Möglichkeit, auf Templates **450** vollständig zu verzichten und stattdessen Berechtigungen **188** in einer Rechteverwaltungssprache (zum Beispiel einer natürlichen Sprache oder Computersprache) zu definieren; ein großer Prozentsatz der Benutzer wird jedoch die benutzungsfreundliche graphische Schnittstelle bevorzugen, die die Templates **450** bereitstellen können, und dafür Einbußen an Flexibilität und mit ihr verbundener Komplexität in Kauf nehmen, solange es um das alltägliche Definieren von Berechtigungen für eine große Anzahl unterschiedlicher Inhalte geht.

[0339] Das exemplarische Rechtetemplate **450** gemäß Fig. 45A (das beispielsweise für Text- und/oder Graphikanbieter angemessen sein kann) definiert eine Anzahl verschiedener Typen für eine konkrete digitale Eigenschaft relevanter Benutzung/Aktionen wie beispielsweise „Titel ansehen", „Zusammenfassung ansehen", „Titel ändern", „weiter vertreiben", „Sicherheitskopie", „Inhalt ansehen" und „Inhalt ausdrucken". Rechtetemplate **450** kann ferner ein „Menü" oder eine Liste mit Optionen bereitstellen, das/die jeweils einem Benutzungstyp entsprechen. Diese verschiedenen Optionen statten den Rechteinhaber mit der Möglichkeit aus, Rechte zu definieren, die andere in Verbindung mit der Eigenschaft ausüben mögen. Die Rechte können beispielsweise umfassen:

- Uneingeschränkte Berechtigung,
- Berechtigung gegen Zahlung,
- Berechtigung in Abhängigkeit von Inhalten,
- Uneingeschränktes Verbot, und
- Verbote und/oder Berechtigungen in Abhängigkeit von anderen Faktoren.

[0340] Rechteinhaber können diese verschiedenen Optionen „ausfüllen" oder zwischen ihnen auswählen, um ein "Rechteprofil" zu definieren, das mit ihrer konkreten Eigenschaft korrespondiert. In diesem Beispiel kann Rechtetemplate **450** Modelle und/oder Ebenen für Rechte, die gegen Zahlung ausgeübt werden können, unterstützen . Solche Preismodelle und -ebenen können verschiedene Arten der geschäftlichen Preisgestaltung wie etwa Einmalzahlungen, Pay-per-View, rückläufige Kosten etc. flexibel definieren. Fig. 45B zeigt ein Beispiel, wie Preismodelle und -ebenen unter Verwendung einer graphischen Schnittstelle vorgegeben werden könnten.

[0341] Das Rechtetemplate **450** in diesem Beispiel kann selbstausführend und/oder „übersetzt" oder automatisch zu einem oder mehreren Regelsätzen **188** kompiliert sein, die die für die Implementierung der Entscheidungen des Rechteinhabers erforderlichen Steuermechanismen bereitstellen. Fig. 45B enthält beispielsweise einen Steuermechanismus **188a** „Titel ansehen", der eine uneingeschränkte Betrachtung des Titels wie durch Rechtetemplate **450** gemäß Fig. 45A vorgegeben ermöglicht. In ähnlicher Weise enthält der exemplarische Steuermechanismus **188** von Fig. 45B ferner Regelsatzelemente **188(2)** ... **188(N)**, die mit anderen Rechten und Berechtigungen **188** korrespondieren, die der Rechteinhaber auf der Grundlage von Rechtetemplate **450** der Fig. 45A definiert hat.

[0342] In diesem Beispiel kann Rechtetemplate **450** erweiterbar sein. In dem Maße beispielsweise, wie eine neue Technologie neue Vorgänge ermöglicht und/oder hervorbringt, kann Rechtetemplate **450** erweitert werden, um die Bedingungen für neue Vorgänge zu schaffen, gleichzeitig jedoch mit bereits bestehenden Rechtetemplates „aufwärtskompatibel" zu bleiben. Es können verschiedene Rechtetemplates **450** für verschiedene Eigenschaftstypen, verschiedene Teilnehmer der Wertkette etc. verwendet werden, gleichzeitig könnten aber auch bestimmte Rechtetemplates auf mehrere Objekte oder Eigenschaften, mehrere Teilnehmer der Wertkette etc. angewandt werden. Einige Rechtetemplates **450** können übergeordnete Sätze anderer Rechtetemplates sein. So könnte ein übergreifendes Rechte- und Berechtigungstemplate **450** sämtliche möglichen Rechte definieren, die auf eine konkrete Eigenschaft oder Eigenschaftsklasse anwendbar sein könnten, und Sub-Templates könnten ferner definiert werden, um unterschiedlichen Verbrauchern, Verbraucherklassen oder Rechteinhabern beigeordnete Rechte zu

definieren. Auf diese Weise könnte ein Autor beispielsweise ein Sub-Template verwenden, welches von jenem abweicht, das der Händler verwendet. Templates können auch rekursiv sein, d. h. dazu verwendet werden, auf andere Templates zu verweisen (und ähnlich können die Regelsätze, die sie definieren, auf andere Regelsätze verweisen).

[0343] Rechte- und Berechtigungs- Clearinghaus **400** könnte Rechtetemplate **450** teilweise ausfüllen, oder es könnte für die Erstellung und/oder Vervielfachung von Rechtetemplates ein automatischer Vorgang (beispielsweise auf Grundlage der bereits bestehenden Anweisungen des Rechteinhabers) benutzt werden. Rechteinhaber könnten eine graphische Benutzeroberfläche benutzen, um Rechtetemplate **450** zu erstellen (z. B. durch Anzeigen einer Liste mit Optionen auf einem Computerbildschirm und Ausfüllen der gewünschten Optionen mittels eines Maus-Zeigegeräts). In einem weiteren Beispiel könnte ein Rechteinhaber seine Präferenzen unter Verwendung einer Rechteverwaltungssprache definieren, die ein Computer automatisch kompilieren oder auf andere Weise verarbeiten könnte, um Rechtetemplate **450** auszufüllen und/oder den (die) beigeordneten Regelsatz (Regelsätze) **188** zu erstellen.

[0344] Fig. 46 zeigt ein Beispiel für einen Rechte- und Berechtigungs-Clearingvorgang unter Verwendung von Rechtetemplate **450**. In diesem Beispiel definieren Rechte- und Berechtigungs-Clearinghaus **400** und/oder individuelle Rechteinhaber das Rechtetemplate **450** (Fig. 46, Block **452(1)**). Die Rechte werden hiernach im Rechtetemplate **450** ausgefüllt, um die erteilten und verweigerten Berechtigungen und die beigeordneten Preismodelle und -ebenen (Block **452(2)**) zu definieren. Der Rechteinhaber ordnet die durch das Rechtetemplate definierten Berechtigungen dem Objekt bei (z. B. durch Erstellung eines oder mehrerer Regelsätze **188**, die auf die gesteuerte Eigenschaft verweisen und/oder angewandt werden) (Block **452(3)**). Der Rechteinhaber kann hiernach die Berechtigungen (Regelsatz **188**) zusammen mit oder getrennt von dem Objekt (Block **452(4)**) übermitteln. Rechteinhaber können diese Regelsätze **188** direkt an die Verbraucher **95** (Block **452(5)**) und/oder an Rechte und Berechtigungs-Clearinghaus **400** zur Registrierung und Abspeicherung in einer Datenbank (Block **452(6)**) senden. Das Rechte- und Berechtigungs-Clearinghaus **400** kann den Verbrauchern (Block **452(7)**) solche vorautorisierten Berechtigungen auf Verlangen nach Erhalt von Verbraucheranfragen (Block **452(8)**) bereitstellen.

[0345] Wie oben beschrieben, können Anbieter den Vertrieb solcher vorautorisierten Berechtigungen über das Rechte- und Berechtigungs-Clearinghaus **400** durch den Mechanismus der Bereitstellung eines zusätzlichen „Vertriebs-Steuermechanismus" steuern, der den Vertriebsvorgang lenkt und/oder steuert.

Zertifizierende Behörde

[0346] Fig. 47 zeigt ein Beispiel für ein Commerce Utility System **500** vom Typ einer zertifizierenden Behörde. Zertifizierende Behörden und Dienste können im Allgemeinen digitale Dokumente erstellen, die eine bestimmte Tatsache „zertifizieren", bestätigen und/oder belegen. Solche Tatsachen umfassen beispielsweise die Identifikation und/oder die Zugehörigkeit zu einer konkreten Klasse wie einer Organisation, Altersgruppe, die Inhaberschaft eines bestimmten Typs eines Berechtigungsnachweises, die Zugehörigkeit zu einer oder mehreren Gerichtsbarkeiten und/oder die Inhaberschaft eines oder mehrerer zertifizierter, über einen bestimmten Zeitraum bzw. bis zu einem bestimmten Datum befristeter Rechte für die Benutzung von Inhalten und/oder Vorgängen.

[0347] Konkreter kann eine zertifizierende Behörde in Übereinstimmung mit den vorliegenden Erfindungen eine beliebige Kombination aus den folgenden vorteilhaften Merkmalen und Funktionen, beispielsweise in Form von Zertifikaten, bereitstellen:

- Elektronische Zertifizierung von Informationen, die mit Regeln und/oder Steuermechanismen benutzt, bzw. von diesen benötigt werden, wie etwa Authentifikation, Identität, Zugehörigkeit zu einer Klasse und/oder andere Identitätsattribute und/oder eine andere Umgebung einschließlich der automatischen Zertifizierung dieser Informationen auf der Grundlage der Quelle (beispielsweise eine oder mehrere Identitäten zertifizierter Anbieter) und/oder Klassen dieser Informationen.
- Bereitstellung einer vertrauenswürdigen Zertifikation darüber, dass ein Verbraucher oder Wertkettenteilnehmer ist, was er zu sein vorgibt und/oder einer oder mehreren konkreten Gruppen, Klassen und/oder Organisationen angehört.
- Bereitstellung einer vertrauenswürdigen Zertifikation darüber, dass eine Gruppe Wertkettenteilnehmer in ihrer Gesamtheit ist, was die Teilnehmer zu sein vorgeben, wobei mehrere Zertifikate verschiedener Parteien in aggregierter Form überprüft werden, wobei ein solches Aggregat bestimmter Zertifikate unter bestimmten Umständen erforderlich ist, damit Inhalte benutzt und/oder ein oder mehrere Regelvorgänge ausgeführt werden können.
- Automatische Erstellung eines Zertifikats, das eine Wertkette oder einen Abschnitt daraus authentifiziert, als Ergebnis des Zusammenfließens mehrerer bestimmter Zertifikate.
- Unter Verwendung von Regeln und Steuermechanismen Vorauswahl zulässiger Zusammenstellungen von mehreren Parteien stammender Zertifikate, die ein Zertifikat bilden können, das eine bestimmte Gruppe zertifizierter Parteien virtuell repräsentiert und bei Vorliegen bestimmter

Zertifikate zwei oder mehr im voraus bestimmte Parteien und/oder Parteien identifiziert, die ein bestimmtes Kriterium erfüllen – z. B. ausreichender Transaktionsumsatz, ausreichende Kreditwürdigkeit etc. – es kann automatisch ein neues Zertifikat generiert werden und als ein zusammengesetztes Zertifikat fungieren, das das kollektive und koordinierte Vorhandensein mehrerer Parteien zertifiziert, wobei dieses Zertifikat verschiedenen Regeln und Steuermechanismen beigeordnet werden kann, wodurch bestimmte elektronische Aktivitäten wie die Benutzung von Inhalten und/oder Steuervorgängen beispielsweise beim elektronischen Datenaustausch mit mehreren Parteien, beim Vertrieb von Inhalten, in einem Handelssystem und/oder in Finanzgeschäftsystemen ermöglicht werden.

• Generierung eines oder mehrerer Zertifikate mindestens teilweise als Ergebnis einer durch Regeln und Steuermechanismen geregelten Erstellung von Zertifikaten, wobei das dergestalt generierte oder die dergestalt generierten Zertifikate beispielsweise im Ergebnis sicherer Regeln und Steuermechanismen auf Grundlage einer oder mehrerer Anweisungen nach der Erfüllung bestimmter erforderlicher Kriterien hergestellt wird (werden) wie etwa bestimmte Aktivitäten jeder von mehreren Parteien, z. B. die Bereitstellung eines oder mehrerer Zertifikate und/oder einer oder mehrerer Vollmachten und/oder Benutzungsaktivität und/oder Gutschrift und/oder Zahlungsaktivität und/oder Berichterstattungs-Aktivität und/oder Aktivität des VDE-gestützten elektronischen Abschlusses von Vereinbarungen (einschließlich beispielsweise Aktivitäten elektronischer Verhandlungen).

• Zertifizierung anderer Unterstützungsleistungen (z. B. Finanz-Clearinghäuser, Usage-Clearinghäuser, Rechte und Berechtigungs-Clearinghäuser, Transaktionsbehörden und andere zertifizierende Behörden etc.).

• Zertifizierung auf der Grundlage eines anderen Zertifikats (z. B. Identität) und einer automatischen sicheren Datenbankrecherche, die lokal, in einer verteilten Datenbankanordnung oder rechnerfern erfolgen kann.

• Bereitstellung nichtautomatischer (i. e. mindestens teilweise manuell oder halbautomatisch ausgeführter) Dienste, die zusätzlich zu automatischen Diensten der Ausstellung abhängiger Zertifikate auf der Grundlage physischer Belege elementarere Zertifikate (z. B. Identität Zertifikate) ausstellen.

• Kann asymmetrische Kryptographie, symmetrische Kryptographie und/oder sichere virtuelle VDE-Netzwerke verwenden, um digitale Zertifikate zu unterstützen, z. B. zu erstellen.

• Kann Zertifikate ausstellen, die den Kontext für eine Benutzung von Rechten in einer automatischen, vertrauenswürdigen, verteilten, nach dem Peer-to-Peer-Prinzip arbeitenden sicheren elektronischen Umgebung unterstützt, die eine Kette der Verarbeitung und Steuerung unterstützt.

• Wie auch bei anderen Diensten des Distributed Commerce Utility, Unterstützung einer unbegrenzten Mannigfaltigkeit unterschiedlicher Geschäftsmodelle und Szenarien mithilfe einer universellen, wieder verwendbaren, programmierbaren, verteilten, modularen Architektur.

• Kann Zertifikate ausstellen, die Regelsätze mit Elementen unterstützen, deren Gebrauch vom Vorhandensein und/oder Nichtvorhandensein spezifischer und/oder von Klassen abhängiger und/oder unspezifischer ein oder mehrerer digitaler Zertifikate abhängt, die bestimmte Tatsachen nachweisen, wobei unterschiedliche Anforderungen bezüglich des Vorhandenseins oder Nichtvorhandenseins von Zertifikaten in Bezug auf unterschiedliche Fragen nebeneinander existieren können.

• Kann ein oder mehrere Zertifikate ausstellen, die mit bedingten elektronischen Regelsätzen kooperieren, um bestimmte Rechte nur bestimmten Verbrauchern und/oder anderen Wertkettenteilnehmern einschließlich beispielsweise Verbrauchern zu gewähren.

• Ersatz ausgelaufener Zertifikate und Unterstützung eines ausgereiften Zeit- und/oder Benutzungs- und/oder anderen Ereignis-gesteuerten Ablaufs (einschl. der Annullierung) von Zertifikaten, wobei beispielsweise die Kriterien für einen solchen Ablauf auf der Grundlage spezifischer Zertifikate, Zertifikatklassen, spezifischer Benutzer und/oder Benutzerklassen, Benutzerknoten etc. variieren können.

• Hinterlegung und Verteilung einschließlich der selektiven Verteilung an verteilte Knoten von Sperrlisten-Informationen, auf der Grundlage beispielsweise von verteilten Knotenprofilen und/oder Regeln und Steuermechanismen.

• Zeitlich gesteuerte, nach einem anderen Ereignis gesteuerte Verteilung von Sperrlisten-Daten auf interoperable Peer-to-Peer-vernetzte Knoten des Distributed Commerce Utility, wobei Informationen in Übereinstimmung mit vereinbarten Anforderungen für Sperrlisten-Informationen selektiv auf einen oder mehrere bestimmte Knoten verteilt werden und/oder wobei Sperrlisten-Informationen nichtselektiv auf bestimmte ein oder mehrere Knoten verteilt werden.

• Empfang in elektronischen Regelsätzen enthaltener Vollmachten von der sicheren Verarbeitungs- und Steuerungskette.

• Verteilung von Funktionen einer zertifizierenden Behörde in einem Netzwerk oder anderen System (beispielsweise ist jeder Verbraucherknoten in Bezug auf bestimmte Zertifikat-Arten eine potentielle zertifizierende Behörde; Eltern können die Vollmacht erhalten, Zertifikate für ihre Kinder auszustellen).

• Hierarchische Organisation von zertifizierenden Behörden einschließlich Schaffung der Möglichkeit einer automatischen Verifizierung mancher zertifizierenden Behörden (d. h. der von ihnen ausgestellten Zertifikate und beigeordneten Bestimmungen mit Hinblick auf Vertrauenswürdigkeit, Verwendbarkeit etc.) durch Hinzuziehung von Zertifikaten, die durch andere zertifizierenden Behörden mindestens teilweise für diesen Zweck ausgestellt wurden.
• Erteilung von Vollmachten und/oder Bereitstellung von Diensten für oder in Verbindung mit einem oder mehreren verteilten untergeordneten Clearinghäusern einer verteilten zertifizierenden Behörde, deren Vorgänge logisch und/oder physisch anderenorts stattfinden können, wie etwa innerhalb eines Unternehmens oder einer Behörde und/oder in einer oder mehreren Gerichtsbarkeit(en), und/oder die Teilbereiche der geschäftlichen Gesamttätigkeit eines übergeordneten Clearinghauses einer verteilten zertifizierenden Behörde abdecken, das Funktionen des Rechteclearings in einem System oder Netzwerk verteilt und/oder anderweitig autorisiert.
• Jeder Verbraucherknoten und/oder bestimmte oder alle anderen Wertkettenteilnehmer-Knoten können potentiell den Clearingdienst einer verteilten zertifizierenden Behörde unterstützen, der seine eigenen, sicheren Zertifikate initiiert und in der Umgebung des Clearinghaus-Gesamtnetzwerks arbeiten, einschließlich der Clearinghaus-Interoperation mit interoperablen Knoten eines oder mehrerer anderer Teilnehmer und, wie auch an anderer Stelle in dieser Liste, sämtlicher Aktivitäten, die beispielsweise VDE-Techniken wie jeweils anwendbar einsetzen.
• Bereitstellung einer Kontrolle der Haftungsakzeptanz (i. e. für die Versicherung digitaler Zertifikate auf der Grundlage des vom Aussteller akzeptierten Haftungsbetrags), kann die sichere Hinterlegung von Informationen in Bezug auf diese Haftungsakzeptanz und die Bereitstellung von Nachrichten an den Empfänger solcher Zertifikate in Bezug auf den durch solche Zertifikate gewährten Haftungsschutz umfassen und kann ferner Empfänger solcher versicherten Zertifikate umfassen, die beispielsweise auf dem Wege einer expliziten VDE-verwalteten elektronischen Annahme oder auf dem Wege einer impliziten Annahme per Weiterführung jede Haftung über den versicherten Beträgen akzeptieren.
• Kann hierarchisch, nach dem Peer-to-Peer-Prinzip oder in einer kombinierten Form organisiert sein wobei die Verantwortung für Aktivitäten der zertifizierenden Behörde für verschiedene Handelsmodelle und/oder Aktivitäten und/oder Wertketten auf verschiedene Weise verteilt sein kann, wobei eine bestimmte oder mehrere Parteien beispielsweise in einem Fall oder mehreren Fällen hierarchisch anderen Parteien übergeordnet, in einem anderen Fall oder mehreren anderen Fällen jedoch hierarchisch ein Peer oder untergeordnet sein kann (können), d. h. die Beziehung zwischen Teilnehmern ist programmierbar und kann dergestalt eingerichtet (und nachträglich verändert) werden, dass für bestimmte gewerbliche Tätigkeiten, Wertketten oder Modelle eine oder mehrere gewünschte Konfiguration(en) der zertifizierenden Behörde entstehen.

[0348] Fig. 47 zeigt eine exemplarische zertifizierende Behörde **500** aus prozessualer Sicht. In diesem Beispiel erstellt zertifizierende Behörde **500** digitale Dokumente, hier Zertifikate **504**, die bestimmte Tatsachen wie etwa eine Identität oder Zugehörigkeit zu einer Klasse „zertifizieren". Beispielsweise kann eine vertrauenswürdige dritte zertifizierende Behörde **500** eine sichere digitale Garantie darüber ausstellen, dass eine Verbraucherin ist, wer sie zu sein vorgibt bzw. bestimmte Merkmale, Attribute, Zugehörigkeit zu Klassen, oder ähnliches aufweist. Beispielsweise können einige Attribute eine Zugehörigkeit zu einer bestimmten Klasse kenntlich machen (z. B. sämtliche Beschäftigte eines bestimmten Unternehmens), vor einem bestimmten Datum geborene Personen, Personen mit einer bestimmten körperlichen Behinderung, Mitglieder der Fakultät, des Verwaltungsorgans oder der Studentenschaft eines College oder pensionierte ehemalige Armeeangehörige.

[0349] In diesem Beispiel werden die durch zertifizierende Behörde **500** ausgestellten digitalen Zertifikate **504** als Übermittler der Umgebung von Rechtebenutzung und Transaktionsautorisierung verwendet. Wie in der Offenbarung des Patents von Ginter et al. beschrieben, sind Zertifikate **504** in der virtuellen Verteilungsumgebung besonders wirksam, da sie Umgebungen für die Rechtebenutzung bereitstellen. So kann etwa eine klassenbasierte Benutzung von Zertifikaten und die automatisierte, verteilte Steuerung der Rechte im Handel die Effizienz vertrauenswürdiger Netzwerke grundlegend verbessern. Angenommen beispielsweise, ein Herausgeber von Inhalten möchte Abonnenten einer wissenschaftlichen Zeitschrift kommerzielle Preise berechnen, sofern diese keine Hochschulbildung haben, und ist bereit, Studenten und Lehrkräften eines College und einer Universität einen Nachlass von 20% zu gewähren. Durch eine vertrauenswürdige zertifizierende Behörde **500** ausgestellte digitale Zertifikate **504** können dazu verwendet werden, in der Umgebung eines verteilten elektronischen Netzwerks automatisch zu garantieren, dass nur solche Personen von dem Nachlass Gebrauch machen können, die auch wirklich einen Anspruch darauf haben (in diesem Beispiel sind dies jene, die als Angehörige einer Hochschuleinrichtung ein Zertifikat besitzen).

[0350] In dem in Fig. 47 gezeigten Beispiel kann die zertifizierende Behörde **500** die folgenden globalen

Funktionen ausführen:

- Erfassen von Tatsachen und Überprüfen **522**,
- Generieren von Zertifikaten **524**
- Pflegen der Sperrlisten **526**,
- Verteilen der Zertifizierungs- und Sperrliste **528**,
- Authentifizierung **530**,
- Erneuern von Zertifikaten **532**,
- Autorisierung **534**,
- Replikation **536**,
- Propagierung **538**, und
- Archivieren **554**.

[0351] Zertifizierende Behörde **500** kann den Nachweis **502** als Grundlage für die Ausstellung digitaler Zertifikate **504** ausstellen. In diesem Beispiel kann der Nachweis **502** weitere digitale Zertifikate **504'** (z. B. derart, dass ein Zertifikat auf einem anderen aufbaut) einschließen. Die Funktion des Erfassens von Tatsachen und des Überprüfens **522** kann diesen Nachweis **502** sowie zusätzliche Daten bezüglich der Vertrauenswürdigkeit **540** (z. B. Daten, die kompromittierte oder kürzlich missbräuchlich verwendete Zertifikate betreffen) erfassen. Die Funktion des Generierens von Zertifikaten **524** kann anhand dieses Prozesses des schnellen Erfassens und Überprüfens **522** neue digitale Zertifikate **504** generieren. Die Verteilungsfunktion **528** kann daraufhin die neuen digitalen Zertifikate **504** verteilen und Rechnungen **542** ausstellen, um eine zertifizierende Behörde für den Aufwand und die Verantwortung zu entschädigen, die mit dem Ausstellen des Zertifikats verbunden sein können.

[0352] Zertifizierende Behörde **500** kann auch eine Sperrliste **542** führen, die auf Daten zur Vertrauenswürdigkeit **540** basiert, die zum Beispiel Zertifikate anzeigt, die kompromittiert wurden oder die angeben, dass kürzlich zertifizierte Tatsachen nicht mehr gültig sind (zum Beispiel war Herr Smith bislang Professor an der Stanford University, ist nun aber nicht mehr an der Universität angestellt). Die Funktion für das Pflegen der Sperrliste **526** ist wichtig, damit ein Mechanismus bereitgestellt wird, der sicherstellt, dass „falsche" Zertifikate nicht weiter verwendet werden können, sobald festgestellt wurde, dass sie nicht mehr „falsch" sind. Zertifikate **504**, die von zertifizierender Behörde **500** ausgestellt wurden, können ablaufen, und die zertifizierende Behörde kann (zum Beispiel gegen eine Gebühr) ein kürzlich ausgestelltes Zertifikat erneuern, indem die Funktion für das Erneuern von Zertifikaten **532** ausgeführt wird. Die zertifizierende Behörde **500** kann ein Protokoll oder eine Datenbank der von ihr ausgestellten Zertifikate unterhalten, und diese Datenbank kann verteilt sein – dabei können die Replikationsfunktion **536** und die Propagierungsfunktion **538** verwendet werden, um die Datenbank exakt und effizient an einer Anzahl von verschiedenen Orten zu verteilen.

[0353] Fig. 48 zeigt einen exemplarischen Aufbau einer zertifizierenden Behörde **500**. In diesem Beispiel kann die zertifizierende Behörde **500** eine Einrichtung für sicheren Datenverkehr **544**, einen Verschlüsselungs-/Entschlüsselungsprozessor **546**, ein Fakturierungssystem **548**, einen Schlüsselgenerator **550**, einen Abfragemechanismus **552** sowie ein elektronisches Archiv **554** einschließen. In diesem Beispiel wird die Einrichtung für den sicheren Datenverkehr **544** verwendet, um mit den anderen elektronischen Geräten **100** und/oder anderen Commerce Utility Systemen **90** zu kommunizieren. Das elektronische Archiv **554** speichert Schlüssel, Zertifikate **504** und weitere für die Aufgabe der zertifizierenden Behörde **500** benötigte Daten. Der Verschlüsselungs-/Entschlüsselungsprozessor **546** wird verwendet, um unter Verwendung leistungsfähiger Verschlüsselungsverfahren digitale Zertifikate **504** zu erstellen. Fakturierungssystem **548** stellt Rechnungen **542** aus. Abfragemechanismus **552** wird verwendet, um das elektronische Archiv **554** abzufragen. Schlüsselgenerator **550** wird verwendet, um kryptographische Schlüssel zu generieren, welche die zertifizierende Behörde **500** für das Ausführen ihrer Aufgabe benötigt.

[0354] Fig. 49 zeigt einen exemplarischen Ablauf der Funktion einer zertifizierenden Behörde. In diesem Beispiel kann ein Herausgeber einen sicheren elektronischen Container **152** an einen Verbraucher **95** senden. Um bestimmte Erlaubnisse **188a** in sicherem Container **152** zu verwenden, kann es sein, dass der Verbraucher **95** ein Zertifikat von einer zertifizierenden Behörde **500** benötigt, das einen bestimmten, den Verbraucher betreffenden Sachverhalt zertifiziert (z. B. dass der Verbraucher Bürger der Vereinigten Staaten ist, dass der Verbraucher ein pensioniertes Mitglied der Streitkräfte ist, dass der Verbraucher über 18 Jahre alt ist etc.). Der Verbraucher kann eine Anfrage **502** über das Ausstellen eines entsprechenden Zertifikats an die zertifizierende Behörde **500** richten. Die zertifizierende Behörde kann den Nachweis **502**, den der Verbraucher **95** oder ein Dritter vorlegen kann, überprüfen und das benötigte digitale Zertifikat **504** für den Verbraucher ausstellen, sobald die Anforderungen der zertifizierenden Behörde **500** erfüllt sind. Dieses digitale Zertifikat **504** kann nicht nur mit dem Regelsatz **188a** des Herausgebers verwendet werden, sondern auch mit dem Regelsatz anderer Rechteinhaber, die eine Zertifizierung desselben Sachverhaltes fordern und die zugestimmt haben, der zertifizierenden Behörde **500** als Behörde für das Ausstellen von Zertifikaten zu vertrauen.

[0355] Zertifizierende Behörde **500** kann mit Verbraucher **95** unter Verwendung eines sicheren Containers **152** kommunizieren. Sie kann einen Regelsatz **188b** mit Zertifikat **504** erstellen und bereitstellen. Dieser Regelsatz **188b** kann bestimmte Aspekte der Verwendung des Zertifikats **504** regeln (z. B. darf es nicht weiter gegeben und/oder verändert werden)

und/oder eine Verarbeitungs- und Steuerungskette für das Ausstellen von weiteren abhängigen Zertifikaten festlegen (z. B. geben Eltern die Erlaubnis, dass Zertifikate an ihre Kinder ausgegeben werden).

[0356] Eine zertifizierende Behörde **500** kann „bevollmächtigt" sein, Zertifikate im Namen einer anderen auszustellen – wie etwa zum Beispiel innerhalb einer von einem oder mehreren elektronischen Regelsätzen **188** festgelegten Verarbeitungs- und Steuerungskette. Das Verteilen der zertifizierenden Behörde **500** auf eine Anzahl von verschiedenen elektronischen Geräten hat bestimmte Vorteile, zum Beispiel im Bezug auf die Effizienz. Fig. 50 zeigt ein nützliches Beispiel dieses Szenarios für das verteilte Ausstellen von Zertifikaten.

[0357] Fig. 50 zeigt, dass ein Rechteinhaber **164** (und/oder ein Rechte- und Berechtigungs-Clearinghaus **400**) eine zertifizierende Behörde **500** auffordern kann (z. B. durch das Ausgeben von elektronischen Regeln **188a** innerhalb eines sicheren Containers **152a**), digitale Zertifikate **504(1)** an akkreditierte Hochschulen wie etwa Institution **1060** auszugeben. Regelsatz **188a** kann die Richtlinien und Verfahrensweisen einrichten, die benötigt werden, um sicher zu stellen, dass eine bestimmte Institution tatsächlich ordnungsgemäß akkreditiert ist. Auf Grundlage elektronischer Regeln **188a** und des von der Einrichtung **1060** ausgestellten Nachweises **502** kann die zertifizierende Behörde **500** ein digitales Zertifikat **504A** ausstellen, das als Nachweis für die Akkreditierung dient.

[0358] Es kann sein, dass ein Student, Mitglied des Lehrkörpers und/oder Angestellter der Institution **1060** ein weiteres Zertifikat vorlegen müssen, das die Tatsache attestiert, dass er oder sie ein Mitglied der Institution **1060** ist, um Zertifikat **504A** zu nutzen. Anstatt dass die zertifizierende Behörde **500** ein zusätzliches Zertifikat **504** an jeden Studenten, jedes Mitglied des Lehrkörpers und jeden Angestellten der Institution **1060** ausgeben muss, kann es effizient und/oder wünschenswert sein, dass jede Institution **1060** ein Zertifikat **504A** besitzt, um abhängige Zertifikate **504(2)** für den eigenen Lehrkörper, das Personal und die Studenten auszustellen. Zum Beispiel kann Institution **1060** eine aktuelle Liste aller Studenten, Mitglieder des Lehrkörpers und Angestellten führen. Anstatt bei zertifizierender Behörde **500** jeweils ein einzelnes Zertifikat **504(1)** für jeden Studenten, jedes Mitglied des Lehrkörpers und jeden Angestellten von Institution **1060** anzufordern, kann die Institution diese Aufgabe selbst übernehmen.

[0359] Zum Beispiel kann es sein, dass Institution **1060** sich dafür entscheidet, ihre eigene, verteilte zertifizierende Behörde **500A** zu betreiben. In einem Beispiel kann die zertifizierende Behörde **500** elektronische Regeln **188b** erstellen (die von Rechteinhaber **164** erstellten Regeln **188a** abhängig sind, zum Beispiel), die an die zertifizierende Behörde **500A** der Institution die Berechtigung und die Zuständigkeit übertragen, abhängige Zertifikate **504**(2) innerhalb bestimmter Grenzen (z. B. das Nachweisen einer begrenzten Gruppe von Tatsachen wie etwa zum Beispiel „Diese Person steht offiziell mit der Institution **1060** in Beziehung") auszustellen. Derartige abhängige Zertifikate **504(2)** könnten zum Beispiel Kopien von Zertifikat **504(1)** sein, die einen Zusatz aufweisen, der bestätigt, dass eine bestimmte Person mit der Institution **1060** in Verbindung steht und die ein bestimmtes Ablaufdatum enthalten (z. B. das Ende des laufenden Semesters). Die zertifizierende Behörde **500A** der Institution kann dann derartige abhängige Zertifikate **504(2)** für jedes auf der aktuellen Liste der Mitglieder verzeichnetes Mitglied des Lehrkörpers, jeden Studenten und jeden Angestellten ausgeben.

[0360] Empfänger von Zertifikaten **504(2)** können noch ein weiteres Zertifikat **504** (1) benötigen, das ihre Identität akkreditiert. Das ist so, weil zertifizierende Behörde **500A** Zertifikate **504(2)** ausstellt, die nachweisen, dass eine bestimmte, namentlich genannte Person Mitglied von Institution **1060** ist, jedoch nicht, dass ein bestimmter Empfänger eines derartigen Zertifikats diese Person ist. Es kann sein, dass der Empfänger dieses weitere „Identitätszertifikat" **504(1)** von einer von der Regierung betriebenen zertifizierenden Behörde **500** anfordern muss, wie etwa einer zertifizierenden Behörde eines Bundesstaates oder des Gesamtstaates.

[0361] Rechteinhaber **164** (und/oder ein nicht gezeigtes Rechte- und Berechtigungs-Clearinghaus **400**) können Regelsätze **188c** für digitales Eigentum **166** erstellen, die Nachlässe oder andere Vergünstigungen für diejenigen Personen gewähren, die eine Kombination aus gültigen digitalen Zertifikaten **504** vorlegen können, die deren Mitgliedschaft in der Klasse "akkreditierte Hochschule" belegen. Jeder Student, jedes Mitglied des Lehrkörpers und jeder Angestellter der Einrichtung **1060**, der ein Zertifikat **504(2)** erhalten hat, kann diese Nachlässe oder anderen Vergünstigungen nutzen. Fig. 50A veranschaulicht, wie derartige verschiedene digitale Zertifikate verwendet werden können, um Regeln **188**, die je nach Zertifikat erstellt werden, zu unterstützen, das heißt, Regelsätze, deren Elemente davon abhängen, ob Zertifikate **504** für den Nachweis bestimmter Tatsachen vorliegen oder nicht.

[0362] In diesem in Fig. 50A gezeigten Beispiel schließen einer oder mehr Regelsätze **188c** eine Anzahl von diskreten Regeln **188(1)** ... **188(N)** ein, die zum Beispiel auf dasselbe digitale Eigentum **166** oder Gruppen von Eigentümern angewendet werden. Regel **188(3)** kann zusätzliche und/oder unterschiedliche Rechte für alle Studenten, Mitglieder des Lehr-

körpers und Angestellte der Stanford University bereitstellen.

[0363] In dem in Fig. 50A gezeigten Beispiel können mehrere Zertifikate zusammen verwendet werden, um die angeforderten Zertifikationen bereitzustellen. Zum Beispiel können die in dem Beispiel in Fig. 50 gezeigten Zertifikate **504(1)**, **504(2)**, **504A** zusammen verwendet werden, um zu ermöglichen, dass eine bestimmte Person einen Rabatt nutzt, der für Studenten, Mitglieder des Lehrkörpers und Angestellte von akkreditieren Hochschulen angeboten wird. Zum Beispiel:

- Kann ein Zertifikat **504(1)** die Tatsache belegen, dass ein gewisser John Alexander tatsächlich die Person ist, die er vorgibt zu sein.
- Kann ein weiteres Zertifikat **504A** die Tatsache belegen, dass Stanford University eine akkreditierte Hochschule ist,
- Kann ein weiteres Zertifikat belegen, dass John Alexander im laufenden Semester Student an der Stanford University ist

[0364] Jedes dieser verschiedenen Zertifikate **504** kann von verschiedenen zertifizierenden Behörden **500** ausgestellt werden. Zum Beispiel könnte eine zertifizierende Behörde **500** (z. B. von einer Regierungsbehörde betrieben) ein Zertifikat **504(1)** ausstellen, das die Identität des Verbrauchers zertifiziert, während eine andere zertifizierende Behörde Zertifikat **504(2)** ausstellen kann, das dessen Studentenstatus attestiert, und eine dritte zertifizierende Behörde kann das Zertifikat ausstellen, welches attestiert, dass Stanford eine akkreditierte Universität ist (siehe Fig. 50).

[0365] Als weiteres Beispiel kann ein in Fig. 50A gezeigtes Regelsatzelement **188**(1) Personen, die ihren Wohnsitz in Kalifornien haben, bestimmte Vorteile gewähren. Diese Bedingung kann erfüllt werden, indem der Verbraucher ein digitales Zertifikat **504(3)** vorlegt, das den Wohnsitz (z. B. in Verbindung mit dem „Identitäts"-Zertifikat **504(1)**) zertifiziert. Noch eine weitere in Fig. 50A gezeigte Berechtigung **180(N)** kann durch das Vorlegen eines Zertifikats **504(5)** über die amerikanische Staatsbürgerschaft erfüllt werden. Derartige Zertifikate **504(3)**, **504(5)**, die gewährleisten, dass eine bestimmte Person einer oder mehreren Gerichtsbarkeiten unterliegt (zum Beispiel, ein Einwohner einer bestimmten Stadt, eines Staates, einer Nation oder einer anderen politischen Einheit oder jemand, der dort arbeitet – und aus diesem Grunde der in dieser Einheit erhobenen Umsatzsteuer, Einkommenssteuer und anderen Steuern oder bestimmten Verwaltungsgebühren unterliegt), sind insbesondere nützlich für Geschäftstransaktionen zwischen verschiedenen Bundesstaaten und/oder zwischen verschiedenen Ländern. Zum Beispiel kann eine zertifizierende Behörde **500** ein Zertifikat **504** an ein Finanz-Clearinghaus **200** im Vereinigten Königreich ausstellen. Dieses Zertifikat **504** könnte in Verbindung mit Regelsätzen **188**, die von Rechteinhabern und/oder Rechte- und Berechtigungsclearinghaus **400** erstellt werden, die festlegen, dass nur Finanz-Clearinghäuser des Vereinigten Königreichs **200** autorisiert sind, eine Bezahlung in Pfund Sterling zu akzeptieren. Ein Verbraucher, der in Pfund Sterling bezahlen möchte, kann den Zahlungsvorgang nur abschließen, wenn das jeweilige Finanz-Clearinghaus das jeweilige UK-Zertifikat hat. Dieses UK-Clearinghaus kann dann die jeweiligen Steuern des Vereinigten Königreichs bezahlen, was den Anbieter von der Aufgabe entbindet, bestimmen zu müssen, welche seiner oder ihrer Transaktionen unter die Steuerregelung des Vereinigten Königreichs fallen oder nicht.

[0366] Fig. 50A zeigt auch ein weiteres Zertifikat **504(4)**, das zertifiziert, dass eine bestimmte Person mit einer bestimmten anderen Person verheiratet ist. Um das Zertifikat **504(4)** zu verwenden, kann es auch notwendig sein, das erste, die Identität zertifizierende Zertifikat **504(1)** vorzulegen. Derartige Zertifikate, die eine Beziehung zwischen Einzelpersonen oder zwischen Personen und Organisation zertifizieren, sind nützlich, wenn zum Beispiel Familienmitgliedern erlaubt werden soll, die Zertifikate anderer Familienmitglieder zu verwenden (z. B. kann eine Person einen Nachlass bekommen, der auf den Credentials seines/ihres Partners oder seiner/ihrer Eltern basiert).

[0367] **Fig.** 51-Fig. 51D zeigen exemplarische detaillierte Formate von verschiedenen digitalen Zertifikaten **504**. Das digitale Zertifikat **504(1)** von Fig. 51A kann zertifizieren dass eine Person tatsächlich die Person ist, die sie vorgibt zu sein. Dieses Zertifikat **504(1)** kann zum Beispiel Folgendes einschließen:

- ein Feld **560(1)**, das den Namen der Person feststellt,
- ein Feld **560(2)**, welches das Geburtsdatum der Person angibt,
- ein Feld zur Ablauffrist **560(3)**, das angibt, wann das digitale Zertifikat abgelaufen ist,
- ein öffentlicher Schlüssel **560(4)**, der dem öffentlichen Schlüssel der Person entspricht, ein ID-Code **560(5)** (der in diesem Beispiel ein Hashwert des Feldes für den öffentlichen Schlüssel **560(4)** sein kann), und
- ein Summenprüffeld **560(6)**, das eine Fehlerprüffunktion bereitstellt.

[0368] Das digitale Zertifikat **504(1)** wird in diesem Beispiel von der zertifizierenden Behörde **500** unter Verwendung des nicht-öffentlichen Schlüssels der zertifizierenden Behörde eines öffentlichen Paares aus öffentlichem Schlüssel und geheimem Schlüssel in einem Kryptosystem, wie etwa RSA oder Elgamal verschlüsselt. Der entsprechende öffentliche Schlüssel der zertifizierenden Behörde **500** kann der Öffentlichkeit zugänglich gemacht werden (z. B. durch Ver-

öffentlichen in mehreren öffentlich zugänglichen Seiten des World Wide Web oder in anderen dezentralisierten Zusammenhängen), oder er könnte geheim bleiben und nicht außerhalb geschützter Verarbeitungsumgebungen **154** zugänglich sein. In jedem Fall stellt eine erfolgreiche Verschlüsselung des digitalen Zertifikats **504(1)** für das Anzeigen der ursprünglichen Information des unverschlüsselten Textes in hohem Maße sicher, dass das digitale Zertifikat von der zertifizierenden Behörde **500** ausgestellt wurde (vorausgesetzt, dass der nicht öffentliche Schlüssel der zertifizierenden Behörde nicht kompromittiert wurde).

[0369] Das Feld mit dem Ablaufdatum **560(3)** ist nützlich, da so bei Personen, welche die Überprüfung von Sperrlisten überspringen, zumindest eine gewisse Sicherheit vorliegt, dass ein Zertifikat gültig ist, wenn es in regelmäßigen Abständen erneuert wird. Das Feld mit dem Ablaufdatum **560**(3) stellt einen zusätzlichen Sicherheitsmechanismus bereit, indem es gewährleistet, dass Zertifikate nicht für immer gültig sind – und so weiteren zertifizierenden Behörden **500** ermöglicht, unterschiedliche Paare von kryptographischen Schlüsseln zu verwenden, um eine allgemeine Integrität und Vertrauenswürdigkeit für den Zertifizierungsvorgang bereitzustellen. Das Verändern des Schlüsselpaares der zertifizierenden Behörde **500** verringert die Anreize für einen Angreifer, einen bestimmten Schlüssel zu brechen, da die Menge der durch diesen Schlüssel geschützten Information beschränkt ist und die missbräuchliche Benutzung eines kompromittierten Schlüssels nur für eine beschränkte Zeit möglich ist. Des Weiteren können (derzeit) unerwartete Fortschritte in der Mathematik einige kryptographische Algorithmen nutzlos machen, da diese auf (derzeit) theoretisch unlösbaren Rechnungen beruhen. Ein eingebauter Mechanismus für das Verändern des Schlüssels der zertifizierenden Behörde **500** ermöglicht, dass die Auswirkungen einer derartigen Aufschlüsselung in ihrer Dauer begrenzt sind, wenn neue Algorithmen für erneut ausgestellte Zertifikate verwendet werden (alternativ kann diese Gefahr auch durch das Verwenden mehrerer asymmetrischer Schlüsselpaare, die gemäß verschiedenen Algorithmen erzeugt wurden, um Schlüssel zu signieren und zu validieren, verringert werden wofür jedoch zusätzliche Verschlüsselungszeit benötigt wird).

[0370] Fig. 51B, Fig. 51C und Fig. 51D zeigen weitere Beispiele für digitale Zertifikate, die verschieden Arten von Information enthalten (z. B. Feld für Credentials von Geschäftspersonen **560(7)** im Falle des Zertifikats **504(5)**, Adressfeldinformation **560(8)** im Falle von Zertifikat **504(3)**, und ein Feld für Credentials von Studenten **504(9)** im Falle eines Studentenzertifikats **504(2)**). Diese Zertifikate **504(2)**, **504(3)**, **504(5)** sind über das gemeinsame ID-Feld **560(5)** zu einem Identitätszertifikat **504(1)** gebündelt, und sowohl das Identitätszertifikat als auch das unabhängige Zertifikat sollten im Allgemeinen zusammen vorgelegt werden.

[0371] Fig. 51E zeigt wie ein exemplarisches, von einer Zertifizierungsbehörde ausgegebenes digitales Zertifikat in Verbindung mit einer vertrauenswürdigen Datenbank für eine andere zertifizierende Behörde die Grundlage für das Ausstellen eines weiteren Zertifikats sein kann. Eine zertifizierende Behörde **500A** kann zum Beispiel die Benutzeridentität validieren und das in Fig. 51A gezeigte Identitätszertifikat **504(1)** erstellen. Der Nutzer kann dieses Identitätszertifikat **504(1)** bei einer anderen zertifizierenden Behörde **500B** einreichen, die eine Datenbank **554a** von Personen und/oder Organisationen hat, die ein bestimmtes Attribut aufweisen. Zum Beispiel kann zertifizierende Behörde **500B** von einer professionellen Organisation betrieben werden, die eine interne Datenbank **554a** führt. Zertifizierende Behörde **500B** vertraut den Inhalten der internen Datenbank **554a**, da die zertifizierende Behörde **500B** sie pflegt und aktualisiert.

[0372] Durch das Vergleichen der Identitätsinformation des in Fig. 51A gezeigten Zertifikats mit dem Inhalt der vertrauenswürdigen Datenbank **554a** kann die zertifizierende Behörde **500B** das in Fig. 51B gezeigte Zertifikat ausstellen, ohne dass ein in irgendeiner Form vorliegender physikalischer Nachweis vom Inhaber des in Fig. 51A gezeigten Zertifikats erforderlich ist. Dadurch wird ein wichtiges Problem gelöst, nämlich die Tatsache, dass der Nutzer jedes Mal in Erscheinung treten muss, wenn er ein Zertifikat mit hoher Vertrauenswürdigkeit benötigt – und ermöglicht zudem, dass das Verfahren des Erstellens des zweiten Zertifikats automatisch abläuft.

[0373] Fig. 51E zeigt außerdem, dass das von der zertifizierenden Behörde **500B** ausgestellte Zertifikat **504(2)** (zusammen mit Identitätszertifikat **504(1)**) eine ausreichende Grundlage für eine weitere zertifizierende Behörde **5000** sein kann, ein weiteres Zertifikat **504(3)** auszustellen, das auf seiner eigenen Suchabfrage in einer vertrauenswürdigen Datenbank **554b** beruht.

[0374] Ein weiteres Beispiel wäre ein Unternehmen, das seine Identität dem Secretary of State der Gerichtsbarkeit, unter die es fällt, mitgeteilt hat. Wenn dieses Unternehmen für die Handhabung von Sondermüll akkreditiert ist, könnte es sein Identitätszertifikat **504(1)** von dem Secretary of State (der in diesem Fall die zertifizierende Behörde **500A** umfassen würde) bei der Behörde (zertifizierende Behörde **500B**, die für das Pflegen der Datenbank **554a** verantwortlich ist, in der Unternehmen aufgeführt sind, die aktuell die Genehmigung für die Handhabung von Sondermüll haben) einreichen. Die zertifizierende Behörde **500B** könnte dann ein Zertifikat **504(2)** aus-

stellen, das diese Tatsache auf vollständig automatisierte Art und Weise bestätigt, wenn dies gewünscht wird.

[0375] Füge an dieser Stelle S. 219 Sichere Verzeichnisdienste ein (in Fig. 52 gezeigt)

Zertifizierung, die es Teilnehmern ermöglicht, als Vertreter einer Einheit zu handeln

[0376] Manchmal müssen einer oder mehr Teilnehmer in einer bestimmten Wertkette oder die in einer bestimmten Beziehung zu anderen Teilnehmern stehen, autorisiert werden, im Auftrag der Gruppe der Teilnehmer zu handeln. Zum Beispiel kann es sein, dass verschiedene Parteien wünschen können, basierend auf der Autorisierung von der Partnership oder dem Joint Venture zu handeln, bei der sie Mitglied sind – oder dass alle Teilnehmer innerhalb einer bestimmten Wertkette für die Wertkette als Ganzes handeln müssen. Jeder der Teilnehmer mit einer derartigen Vollmacht der Einheit kann eine Handlungserlaubnis von der Einheit erhalten.

[0377] Die vorliegende Erfindung stellt einen Mechanismus bereit, in dem digitale Zertifikate verwendet werden können, um eine „virtuelle Einheit" zu erstellen, die einer beliebigen Kombination von Teilnehmern eine beliebige Kombination von gleichen oder unterschiedlichen Rechten zuteilen kann, um festgelegte Rechte unter bestimmten kontrollierten Nutzungsbedingungen auszuüben. Insbesondere teilt ein digitales Zertifikat jedem Teilnehmer in einer virtuellen Einheit das Recht zu, im Auftrag der Einheit zu handeln – innerhalb durch die Nutzungsbedingungen festgelegten Einschränkungen und ferner mit beliebigen in den Nutzungsbedingungen definierten Konsequenzen, die durch elektronische Steuermechanismen festgelegt werden, die mit dem Container assoziiert sind.

[0378] Fig. 51F zeigt einen exemplarischen elektronischen Container **152**, der die folgende Information enthält:
einen Wert **564**, der die „virtuelle Einheit" identifiziert,
Signaturen **566(1)**-**566(N)** – jeweils eine für jedes Mitglied der Einheit, weitere, sich auf die Einheit beziehende Daten **568**,
digitale Zertifikate **504(1)**-**504(N)** – jeweils eine für jedes Mitglied der Einheit, und
Steuerungsdaten **188**, die Rechte zuteilen (z. B. Rechte oder Berechtigungen sowie „Nutzungsbedingungen".

[0379] Wert **564** stellt einen Identifikationswert bereit, der die Einheit eindeutig festlegt. Das Feld für „weitere Information" **568** kann weitere, die Einheit betreffende Daten bereitstellen (z. B. den Namen der Einheit, den Namen und die Adresse jedes Teilnehmers, das Ablaufdatum, an dem die Einheit aufhört zu existieren, sowie weitere Informationen). Signaturen **566(1)**-**566(N)** sind wie Unterschriften unter einem Gesellschaftsvertrag – jedes Mitglied der virtuellen Einheit setzt seine oder ihre „Unterschrift" darunter, um anzugeben, dass es unterschreibt, ein Mitglied der Einheit zu sein und dass er in die Bedingungen, die für jeden Teilnehmer gelten, einwilligt.

[0380] Container **152** schließt in diesem Beispiel weiterhin einen elektronischen Regelsatz **188** ein, der Bedingungen, unter denen die Rechte ausgeübt werden dürfen, beschreibt. Regeln **188** legen eines oder mehr Rechte fest, die jedem Teilnehmer zugeteilt werden, einschließlich (in diesem Beispiel) Bedingungen oder Einschränkungen für das Ausüben dieser Rechte. Regeln **188** können dieselben Rechte und/oder Nutzungsbedingungen für jeden Teilnehmer festlegen oder können unterschiedliche Rechte und/oder Nutzungsbedingungen für jeden Teilnehmer festlegen.

[0381] Zum Beispiel können Regeln **188** jedem Teilnehmer in einer virtuellen Einheit das Recht zuteilen, die Funktion einer Zertifizierungsbehörde 500 im Auftrag der Einheit zu übernehmen. In diesem speziellen Beispiel können Regeln **188** es ermöglichen, dass jede Partei der virtuellen Einheit Zertifikate im Auftrag der virtuellen Einheit erstellt – innerhalb der Einschränkungen der Nutzungsbedingungen und ferner mit den in den Nutzungsbedingungen festgelegten Konsequenzen, die durch die Regeln festgelegt sind. Wie oben dargelegt, ist das Recht, Zertifikate auszustellen, nur ein Beispiel – jede Art von einem oder mehreren elektronischen Rechten oder Berechtigungen könnte auf der Grundlage jedes beliebigen Typs von einer oder mehreren elektronischen Nutzungsbedingungen erteilt werden.

[0382] Fig. 51G zeigt ein Beispiel für ein Verfahren des Erstellens des in Fig. 51F dargestellten Containers **152**. In diesem Beispiel können die an der virtuellen Einheit beteiligte Parteien Steuerungsdaten verhandeln, die die gemeinsamen Aktionen regeln, zum Beispiel die elektronischen Verhandlungstechniken, die in **Fig.** 75A-76B der Patentschrift von Ginter et. al. (Fig. 51G, Block **570**) gezeigt werden. Die resultierenden Steuerungsdaten **188** legen „Nutzungsbedingungen" fest, wie etwa die Rechte, die von jedem Teilnehmer in der Einheit ausgeübt werden können, sowie Einschränkungen jedes dieser Rechte (die für jeden Teilnehmer einzeln festgelegt werden können).

[0383] Der Teilnehmer, der die Erstellung von digitalem Container **152** initiiert (eigentlich tut dies die geschützte Verarbeitungsumgebung **154** des Teilnehmers) kann einen zufälligen Wert auswählen, der als Wert für das Identifizieren der Einheit (Fig. 51G, Block **572**) verwendet wird. Die PPE (protected processing environment, geschützte Verarbeitungsum-

gebung) des Teilnehmers kann als nächstes die Zertifikationsdaten für die virtuelle Einheit erstellen, indem der Wert für das Identifizieren der Einheit **564** mit anderen Daten **568** verknüpft wird (Fig. 51G, Block **574**). Die PPE des Teilnehmers **154** kann als nächstes die Daten über das Zertifikat der virtuellen Einheit signieren, um anzuzeigen, dass er einwilligt, ein Mitglied der virtuellen Einheit zu sein sowie dass er in die Steuerungsdaten zu den Nutzungsbedingungen **188** (Fig. 51G, Block **576**) einwilligt.

[0384] Die PPE des Teilnehmers **154** kann dann elektronischen Container **152** erstellen und in diesem die Steuerungsdaten **188** ablegen, die Information über das Zertifikat der virtuellen Einheit **564**, **566**, **568** sowie das eigene Zertifikat des Teilnehmers **504**, indem sie einen kryptographischen Schlüssel festlegt, den der Teilnehmer verwenden darf, um Rechte auszuüben (Fig. 51G, Block **578**). Der Teilnehmer kann dann festlegen, ob noch weitere Teilnehmer auf dem Zertifikat der Einheit erscheinen sollen (Fig. 51G, Entscheidungsblock **580**). Wenn ja, kann der Container **152** an einen anderen Teilnehmer, der Mitglied der virtuellen Einheit ist (Fig. 51G, Block **582**) übertragen werden, und dieser nächste Teilnehmer kann darauf zugreifen und ihn validieren (Fig. 51G, Blöcke **584**, **586**). Die nächste Teilnehmerin kann in gleicher Weise die Zertifizierungsinformation der virtuellen Einheit signieren, indem er seine Signatur **566(2)** der Liste hinzufügt – und damit angibt, dass sie ebenfalls mit den Regeln **188** sowie damit, der virtuellen Einheit beizutreten, einverstanden ist (Fig. 51G, Block **588**). Diese neue Information wird verwendet, um Zertifizierungsdaten der Einheit **564**, **566**, **568** (Fig. 51G, Block **590**) zu ergänzen und/oder zu ersetzen. Dieser nächste Teilnehmer fügt ebenfalls sein eigenes Zertifikat **504(2)** zu dem Container **152** hinzu (Fig. 51G, Block **592**).

[0385] Schritte **580**-**592** können wiederholt werden, bis Container **152** von jedem Teilnehmer innerhalb der virtuellen Einheit signiert wurde ("Nein"-Ausgang des Entscheidungsblocks **580**). Der fertige Container **152** kann dann an alle Teilnehmer übertragen werden (Fig. 51G, Block **594**).

[0386] Fig. 51H zeigt ein exemplarisches Verfahren, das ein Teilnehmer der virtuellen Verarbeitungsumgebung anwenden kann, um Rechte im Auftrag der virtuellen Einheit und basierend auf den in Fig. 51F gezeigten Regeln **188** auszuüben. Das in Fig. 51H gezeigte exemplarische Verfahren wird von der geschützten Verarbeitungsumgebung **154** des Teilnehmers – basierend auf einer Anfrage ausgeführt. Die geschützte – Verarbeitungsumgebung **154** des Teilnehmers schreibt eine Audit-Aufzeichnung (Fig. 51H, Block **594a**) und evaluiert dann die Anfrage unter Verwendung der durch Regeln **188** festgelegten Nutzungsbedingungen (Fig. 51H, Block **594b**). Wenn die Anfrage durch die Regeln **188** erlaubt ist ("JA"-Ausgang des Entscheidungsblocks **594c**, Fig. 51H), greift die geschützte Verarbeitungsumgebung **154** des Teilnehmers über den Container **152** auf den Wert der virtuellen Einheit **564** zu (Fig. 51H, Block **594d**) und verwendet die mit den Nutzungsbedingungen assoziierten Steuerungsdaten **188**, um die Anfrage auszuführen und geeignete Konsequenzen durchzuführen (Fig. 51H, Block **594e**). In einem Beispiel kann die geschützte Verarbeitungsumgebung **154** des Teilnehmers die Funktion einer zertifizierenden Behörde **500** im Auftrag der virtuellen Einheit haben, indem sie ein digitales Zertifikat **504** gemäß den Nutzungsbedingungen ausstellt – durch digitales Signieren des digitalen Zertifikats durch das Verschlüsseln des Werts für das Identifizieren der Einheit **564** mit einem kryptographischen Schlüssel, der dem eigenen Zertifikat des Teilnehmers **504** innerhalb des Containers entspricht und dadurch, dass sie das digitale Zertifikat zu einem Teil eines neu ausgestellten Zertifikats macht. Das Beispiel kann dann zusätzliche Auditdaten **594H** schreiben, die über die durchgeführte Aktion Bericht erstattet.

[0387] Wenn die angeforderte Aktion nicht durch die Regeln **188** erlaubt ist (Fig. 51H, "Nein"-Ausgang des Entscheidungsblocks **594c**), dann bestimmt das in Fig. 51H gezeigte beispielhafte Verfahren, ob der Fehler kritisch ist (Entscheidungsblock **594f**).

[0388] Wenn der Fehler kritisch ist („JA"-Ausgang des Entscheidungsblocks **594f**), dann kann das Verfahren eine weitere Verwendung der Information in Container **152** (Block **594g**) verhindern, es schreibt zusätzliche Auditdaten auf (Block **594h**) und bricht dann ab (Fig. 51H, Block **594i**). Wenn der Fehler nicht kritisch ist („NEIN"-Ausgang des Entscheidungsblocks **594f**), dann schreibt die geschützte Verarbeitungsumgebung **154** zusätzliche Auditdaten (Block **594h**) auf und kann dann diese Aufgabe abschließen (Fig. 51H, Block **594i**).

[0389] Die in Fig. 51F-Fig. 51H gezeigten Verfahren und Techniken haben eine Vielzahl von verschiedenen Anwendungsmöglichkeiten. Als Beispiel stelle man sich vor, dass ein erster Herausgeber ein adaptiertes Werk herausgibt, das eigene Inhalte sowie Inhalte eines zweiten Herausgebers enthält. Die beiden Herausgeber können eine virtuelle Einheit bilden, die es dem ersten Herausgeber ermöglicht, im Auftrag der Einheit zu handeln – jedoch nur gemäß den Nutzungsbedingungen, die von beiden Partnern ausgehandelt und vereinbart wurden. Zum Beispiel kann es sein, dass der zweite Herausgeber dem ersten Herausgeber erlauben möchte, die Inhalte des zweiten Herausgebers nachzudrucken und es den Verbrauchern **95** erlauben möchte, Auszüge sowie Anthologien aus diesem Inhalts zu erstellen – jedoch nur, wenn die Verbraucher ein entsprechendes Zertifikat **504** vorlegen, dass von der virtuellen Einheit

ausgestellt wurde und das als Nachweis dafür dient, dass der Verbraucher dieses Recht ausüben darf. Zum Beispiel kann es sein, dass lediglich bestimmte Abonnenten mit bestimmten Eigenschaften ein entsprechendes Zertifikat **504** bekommen können. Die oben gezeigten Techniken ermöglichen es dem ersten Herausgeber, Zertifikate **504** an Abonnenten im Auftrag der virtuellen Einheit auszugeben, die sowohl den ersten als auch den zweiten Herausgeber umfasst. Der zweite Herausgeber kann sich sicher sein, dass der erste Herausgeber Zertifikate ausschließlich gemäß den von beiden Herausgebern verhandelten und vereinbarten Nutzungsbedingungen ausstellen wird.

[0390] Ein weiteres Beispiel ist ein Herstellungsverfahren, das mehrere Teilnehmer umfasst. Die durch die Regeln **188** aufgestellten Nutzungsbedingungen können es jedem Teilnehmer der Wertkette in der Wertkette des Herstellungsprozesses ermöglichen, bestimmte Aktionen im Auftrag der Wertkette als Ganzes auszuführen. Zum Beispiel können ein Hersteller von Werkstoffen, ein Zulieferer von fertigen Produkten und die Transportfirma, die Materialien zwischen diesen hin und her transportiert, eine virtuelle Einheit bilden. Diese virtuelle Einheit kann dann einen Regelsatz bei einer Transaktionsbehörde hinterlegen, der ein Verfahren festlegt, welches das Zusammenspiel aller drei Teilnehmer beschreibt. Zum Beispiel kann der gemäß den Nutzungsbedingungen vereinbarte Regelsatz, der auf ihre virtuelle Einheit angewendet werden soll, eine einheitliche Darstellung von benötigten Materialien, Aussehen der fertigen Produkte und Lieferplan ermöglichen, um nur ein Beispiel zu nennen.

[0391] In einem weiteren Beispiel können ein Unternehmen, das Halbleiter herstellt, ein Systemintegrator und drei verschiedene Zulieferer von Software eine virtuelle Einheit bilden, die das Chipdesign des Halbleiterunternehmens, die Simulation und Anwendungen für das Testen von Ausführungen unterstützen. In diesem Beispiel können an jedes Unternehmen, das zu dieser exemplarischen virtuellen Einheit gehört, sowie an Einzelpersonen innerhalb jedes Unternehmens Zertifikate ausgegeben werden. Regelwerke, die zwischen diesen Unternehmen verhandelt wurden, können festlegen, wer auf welche Teile der Softwareanwendungen und assoziierten Datenbanken Zugriff hat und wer Änderungen an der Software und/oder den Daten vornehmen darf. Auf diese Weise kann das Halbleiterunternehmen externen Lieferanten und/oder Zulieferern sowie Einzelpersonen, welche diese externen Firmen vertreten, den Zugriff gewähren. Diese Einzelpersonen können genau soviel Zugriff haben, dass sie üblicherweise auftretende Probleme lösen können und Systemwartungsaufgaben durchführen können. Ihnen können auch zusätzliche Rechte (Autorisierungen) für eine begrenzte Zeit zugeteilt werden, damit sie spezifische Probleme lösen können, für deren Lösung ein Zugriff auf bestimmte ausführbare Dateien und/oder Daten, die ihnen nicht als Standardrechte zugeteilt wurden, erforderlich ist.

[0392] Das Merkmal der virtuellen Einheit der vorliegenden Erfindung stellt teilweise eine Erweiterung dar, die auf den in Ginter et. al. offenbarten Verarbeitungs- und Steuerungstechniken aufbaut. Zum Beispiel können Zertifikate, die gemäß diesem Aspekt der vorliegenden Erfindung hergestellt wurden, Fähigkeiten einer VDE-Verarbeitungs- und Steuerungskette verwenden, um eine Kette von Zertifikaten zu verwalten.

Sichere Verzeichnisdienste

[0393] Fig. 52 zeigt ein Beispiel für einen sicheren Verzeichnisdienst eines Commerce Utility Systems **600**. Sichere Verzeichnisdienste können auf sichere Art und Weise elektronische und/oder sonstige Verzeichnisdaten, wie etwa Namen, Adressen, öffentliche Schlüssel, Zertifikate und Ähnliches bereitstellen. Die Übertragung derartiger Daten (z. B. unter Verwendung der virtuellen Verteilungsumgebung, wie in der bevorzugten Ausführungsform) trägt dazu bei, den Diebstahl von Daten zu verhindern, unterstützt die Sicherung der Vertrauenswürdigkeit und stellt in bedeutsamer Weise eine Unterstützung der Infrastruktur bereit, wodurch die Interaktion zwischen den Teilnehmern in hohem Maße effizient wird.

[0394] Genauer gesagt können gemäß vorliegenden Erfindungen bereitgestellte sichere Verzeichnisdienste die folgenden exemplarischen vorteilhaften Merkmale und Funktionen bereitstellen:

- Sicheres und zuverlässiges Bereitstellen von Verzeichnisdaten basierend auf einer Vielzahl von verschiedenen Parametern, einschließlich unterschiedlicher Klassifizierungsdaten.
- Kann auf sichere Art und Weise eine oder mehrere elektronische Adressen und/oder einen oder mehr weitere Kommunikationswege von Verbrauchern, Anbietern von Inhalten, Clearinghäusern und/oder Dritten basierend auf deren Name, Funktion, Standort und/oder weiteren Attributen bereitstellen.
- Kann einen oder mehrere öffentliche Schlüssel und/oder eines oder mehrere Zertifikate von Verbrauchern, Anbietern von Inhalten, Clearinghäusern und/oder Dritten basierend auf deren Name, Funktion, Standort und/oder weiteren Attributen bereitstellen.
- Schützt und verbirgt gegebenenfalls auf die Identität bezogene Daten und verwaltet gleichzeitig effizient und/oder automatisiert den vertraulichen Datenverkehr von Anfragen und Antworten in sicheren Containern.
- Verwendet dabei sichere Container sowie Regeln und Steuermechanismen, um die Integrität

und die Unversehrtheit von Inhalten zu garantieren.
• Erhält dabei von sicheren Verarbeitungs- und Steuerungsketten Genehmigungen, welche in die elektronischen Regelsätze integriert sind.
• Verteilt dabei Funktionen der sicheren Verzeichnisdienste über das Netzwerk oder ein anderes System (zum Beispiel ist potentiell jeder Verbraucher und/oder anderer Knoten mit einem Teilnehmer der Wertkette ein verteilter Verzeichnisdienst, der seine eigenen Transaktionen sicherer Verzeichnisdienste direkt mit einem oder mehr anderen Teilnehmern unter Verwendung einer VDE wie in der Patentbeschreibung von Ginter et al. beschrieben, initiiert.
• Teilt Berechtigungen zu und/oder stellt Dienste für oder in Verbindung mit einem oder mehr verteilten Sub-Clearinghäusern mit sicheren Verzeichnisdiensten bereit deren Tätigkeiten logisch und/oder physikalisch lokalisiert werden können, wie etwa innerhalb eines Unternehmens oder einer Regierungsbehörde und/oder innerhalb eines oder mehr Gerichtsbarkeiten und/oder Untereinheiten von Dienstleistern des gesamten Hauptgeschäftsbereichs einer übergeordneten Behörde von Verzeichnisdiensten, die sichere Unterstützungsfunktionen direkt verteilt oder Genehmigungen innerhalb eines Systems oder eines Netzwerks genehmigt.
• Jeder Verbraucher und/oder bestimmte oder alle Teilnehmerknoten der Wertkette können potenziell eine Behörde für sichere Verzeichnisdienste unterstützen, die Namensdienste und zugehörige Dienste und Funktionen im Zusammenhang mit dem übergeordneten Netzwerk für die Namensgebung, einschließlich der Interoperation mit einem oder mehr interoperablen Teilnehmerknoten und wie auch sonst in dieser Aufzählung gültig, sämtlichen Aktivitäten, die geeignete VDE-Techniken anwenden, bereit stellt.
• Kann hierarchisch organisiert sein, um Verantwortlichkeiten und Tätigkeiten von sicheren Verzeichnisdiensten für eine Teilmenge des gesamten Verzeichnisses basierend auf Name, Funktion, Standort und/oder anderen Attributen zuzuteilen.
• Kann hierarchisch organisiert sein, um beispielsweise ein Verzeichnis der Verzeichnisse zu erstellen.
• Kann hierarchisch oder auf einer Peer-to-Peer-Struktur basierend aufgebaut sein oder in einer Kombination aus beiden, worin Verantwortlichkeiten von Verzeichnisdiensten auf verschiedene Arten für das Unterscheiden von Verkaufsmodellen und oder Aktivitäten und/oder Wertketten verteilt sein können und worin bestimmte oder mehr Parteien hierarchisch anderen Parteien übergeordnet sein können in einer oder mehr Instanzen und hierarchisch auf gleicher Ebene oder untergeordnet in einer oder mehr Instanzen sein können, das heißt, dass die Beziehung zwischen den Teilnehmern zu einer oder mehr gewünschten speziellen Anordnungen von Verzeichnisdiensten für bestimmte Verkaufsaktivitäten, Wertketten und/oder Modelle programmiert werden und festgelegt (und später geändert) werden kann.

[0395] Fig. 52 zeigt ein Beispiel für einen sicheren Verzeichnisdienst **600** unter dem Gesichtspunkt des Verfahrens. In diesem Beispiel ist sicherer Verzeichnisdienst **600** ein Archiv, das sicher eine Übersicht über die auf Verbraucher, Teilnehmer der Wertkette und/oder elektronische Geräte bezogenen Daten bietet und diese Information auf Grundlage von geeigneten Anfragen sicher bereitstellt. In diesem Beispiel kann sicherer Verzeichnisdienst **600** die folgenden Funktionen bereitstellen:
- Datenbankverwaltung **606**,
- Durchsuchen/Abruf von Datenbanken **608**,
- Replikation von Datenbanken **610**,
- Datenbankpropagierung **612**,
- Authentifizierung **614**, und
- Autorisierung **616**.

[0396] Auf Datenbank **606** kann mittels der Such- und Abrufeinrichtung **608**, die als Quelle von Verbrauchern bereitgestellte Eingabeinformation verwendet und diese verwendet, um relevante Berichte abzurufen, zugegriffen werden. Zum Beispiel kann sicherer Verzeichnisdienst **600** Identitäten **618** von Einzelpersonen, Organisationen, Diensten und/oder Vorrichtungen, elektronische Adressen **620**, Zertifikat **622** und/oder Schlüsseln **624** empfangen. Diese Information kann in Datenbank **606** gespeichert sein.

[0397] Als Antwort auf die Anfragen **602** kann die Such- und Abrufeinrichtung **608** des sicheren Verzeichnisdienstes auf die Datenbank **606** zugreifen, um zusätzliche Information abzurufen (zum die E-Mail-Adresse einer bestimmten Einzelperson oder einer Organisation, den öffentlichen Schlüssel einer bestimmten Einzelperson, die Identität einer Person mit einer bestimmten E-Mail-Adresse, die Identität und die Adresse einer Person mit einern bestimmten öffentlichen Schlüssel etc.).

[0398] Zusätzlich können sichere Verzeichnisdienste **600** Zugriffskontrollen, Audit-Anforderungen und ähnliches zurücksenden. Zum Beispiel kann es notwendig sein, dass ein Benutzer gültige Credentials (z. B. ein Zertifikat **504**) vorlegt, um Zugang zu den internen Mailadressen eines Unternehmens zu haben. Bestimmte in der Datenbank **606** gespeicherte Informationsbereiche können möglicherweise nicht überall zugänglich sein (z. B. die Adresse eines Büros oder eines bestimmten Angestellten, das Verzeichnis mit deren Privatadressen auf den Servern des Unternehmens, etc. oder eine tatsächliche Adresse eines Verbrauchers kann für Personen zugänglich sein, die

ein Zertifikat **504** vorlegen, das von dem Verbraucher, der seine eigene zertifizierende Behörde **500** darstellt, und von keinem sonst, ausgestellt wurde. Diese Regeln können in sicheren Containern festgelegt werden, welche die Daten zu dem sicheren Verzeichnisdienst **600** tragen.

[0399] Wenn die Daten Personen, welche diese angefordert haben, bereitgestellt werden, dann kann es sein, dass sie aufgefordert werden, diese nur auf erlaubte Art und Weise zu verwenden. Zum Beispiel kann es sein, dass sie die Information verwenden dürfen, um E-Mail-Nachrichten zu schreiben, aber nicht um eine physikalische Adresse für eine Mailingliste zu entnehmen. Diese Einschränkungen können durch Regeln **188b** verstärkt werden, die der sichere Verzeichnisdienst **600** mit den bereitgestellten Daten verknüpft.

[0400] Wie in Fig. 53 gezeigt, kann sicherer Verzeichnisdienst **600** eine Datenbank **606** sowie die Such- und Abrufeinrichtung **608** zusätzlich zu einer Einrichtung für den sicheren Datenverkehr **626** bereitstellen. Der Aufbau des sicheren Verzeichnisdienstes **600** kann auf den Fig. 12 und Fig. 13 der Patentschrift von Ginter et al. basieren.

[0401] Fig. 54 zeigt ein Beispiel für ein von einem sicheren Verzeichnisdienst **600** durchgeführtes Verfahren. In diesem Beispiel möchte ein Sender **95(1)** eine Nachricht an einen Empfänger **95(2)** senden. Die Sender und Empfänger sollten elektronische Geräte **100** sein, die Verbrauchern, Clearinghäusern oder ähnlichem gehören. Sender **95(1)** kann eine Adressanforderung **602** an den sicheren Verzeichnisdienst **600** senden, um bestimmte Daten bereitzustellen und andere Daten anzufordern. Als Antwort darauf kann sicherer Verzeichnisdienst **600** die angeforderten Daten für den Sender **95(1)** bereitstellen, der die Daten verwenden kann, um eine Nachricht an den Empfänger **95(2)** zu senden. In diesem Beispiel sind sowohl die Adressanforderung **602** als auch die als Antwort gesendeten Daten **604** in den sicheren elektronischen Containern **152** enthalten, um die Vertrauenswürdigkeit und die Integrität der Anfragen und Antworten zu erhalten. Somit können zum Beispiel externe Datenspione nicht herausfinden, mit wem Sender **95(1)** kommunizieren möchte oder welche Information er oder sie benötigt, um den Datenverkehr durchzuführen und die Verzeichnisantworten können nicht derart manipuliert werden, dass sie die angeforderten Nachrichten an einen anderen Ort weiterleiten. Zusätzlich können Verzeichnisdienste **600** zusammen mit ihren Antworten und/oder Anforderungen Regeln **188** einschließen oder Regeln **188** als Teil ihrer Eingabe erfordern.

Transaktionsbehörde **700**

[0402] Fig. 55 zeigt ein exemplarisches Beispiel für eine Transaktionsbehörde eines Commerce Utility Systems. Diese Erfindungen ermöglichen auch Eigenschaften von sicheren „Transaktionsbehörden", welche die folgenden allgemeinen Funktionen bereitstellen:

- Sicheres Validieren, Zertifizieren und/oder Auditereignisse (einschließlich, zum Beispiel, Authentifizierung, und, zum Beispiel, für Nichtrückweisbarkeit) in einer universellen Transaktion mit Mehrfach-Vorgängen oder einer Kette von Verarbeitungs- und Steuerungsprozessen;
- Sicheres Speichern, Validieren, Zertifizieren und/oder Verteilen von Regelsätzen (einschließlich, zum Beispiel, Authentifizierung, und, zum Beispiel, für die Nichtrückweisbarkeit) in einer universellen Transaktion mit Mehrfach-Vorgängen oder einer Kette von Verarbeitungs- und Steuerungsprozessen;
- Ausgeben von Anforderungen für jede oder alle der Transaktions- und/oder Verfahrensschritte, und
- Gegebenenfalls aktive Teilnahme an der Transaktion oder dem Prozess (z. B. durch das Verwalten, Weiterleiten, Vermitteln, Schlichten, Initiieren etc. einschließlich Teilnahme in Modellen, die gegenseitige Steuerungsverfahren und verteilte, automatisierte Ereignisse für zum Beispiel verteilte Rechentechniken, Prozessmanagement, EDI, Referenzwährung etc.) anwenden.
- Kann Schritte und/oder Übertragungswege zertifizieren, einschließlich das Zertifizieren des korrekten Weiterleitens von elektronischen Daten über Telekommunikationsweichen von Transaktionsbehörden, die geeignet sind, bestimmte Daten zu zertifizieren und wobei Zertifikate zertifizieren, dass einer benötigten Route gefolgt wurde oder nicht und/oder dass das Senden derartiger elektronischer Daten gemäß bestimmten vereinbarten Regeln und Steuermechanismen erfolgte, zum Beispiel, das Erwerben bestimmter Archivierungsdaten und/oder das Nicht-Überschreiten eines Budgets und/oder andere Begrenzungen und/oder Einschränkungen bezüglich, zum Beispiel folgendem: Anzahl von übertragenen Datencontainern in einer bestimmten Zeitspanne, Wert der in einem Währungscontainer enthaltenen (dadurch dargestellten) elektronischen Währung und/oder durch Container über eine gewisse Zeitspanne hinweg, Menge an Geldmitteln die bei einem Kaufautrag ausgegeben werden kann, maßgebende Behörde für Bestellungen, etc.

[0403] Die Transaktionsbehörde kann ganz einfach ein sicherer, aufmerksamer Beobachter und Zertifizierer der elektronischen Transaktion und/oder des Transaktionsschritts sein (in einer Abfolge von globalen Transaktionsschritten), sie kann eine sicherer Moderator einer sicheren Transaktion, bei der viele Parteien beteiligt sind, sein und/oder kann aktiv und direkt bei der elektronischen Transaktion mitwirken.

[0404] Genauer gesagt kann die Transaktionsbehörde gemäß vorliegenden Erfindungen die folgenden vorteilhaften Merkmale und/oder Funktionen bereitstellen:

- Sicheres Aufrechterhalten und Validieren von Ereignisanzeigedaten einer mehrstufigen Transaktion und/oder einer oder mehrere Prozesse einer Verarbeitungs- und Steuerungskette.
- Kann, durch Anforderungen einer Zertifizierung oder Authentifizierung eine Abfolge von Prozessen einer erforderlichen Transaktion und/oder Verarbeitungs- und Steuerungskette basierend auf Komponentendarstellung von Elementen eines Geschäftsprozesses unterstützen, wobei zum Beispiel eine oder mehr Transaktionsbehörden jeweils eines oder mehr Ereignisse bei einem oder mehr „Orten" von Schritten in einer Transaktionsabfolge zertifizieren und/oder authentifizieren.
- Kann einen allgemeinen Regelsatz für Transaktionen aus einer Anzahl von diskreten Teilmengen von Regelsätzen erstellen, die zum Beispiel durch eine Anzahl von verschiedenen Teilnehmern beigesteuert werden.
- Verwendet dabei wechselseitige Verfahren, um erforderliche Transaktionsereignisse zwischen Teilnehmern der Wertkette zu koordinieren, einschließlich zum Beispiel, Abfolge von Ereignissen.
- Erhält dabei Genehmigungen von sicheren Verarbeitungs- und Steuerungsketten, die in die elektronischen Regelsätze integriert sind.
- Kann derart intervenieren, dass sie aktiv Transaktionen und/oder Prozesse der Verarbeitungs- und Steuerungskette leitet.
- Kann den Arbeitsablauf und/oder Prozesse der Verarbeitungs- und Steuerungskette und/oder andere Geschäftsprozesse koordinieren.
- Kann eine automatische und effiziente Verwaltung bereitstellen, die auf einer vertrauenswürdigen, sicheren, verteilten elektronischen Handelsumgebung, einschließlich Zertifizierungs- und/oder Authentifizierungsschritten in verteilten geschützten Daten, EDI, Finanztransaktionen und oder Aktivitäten von Wertketten von Handelssystemen, welche die Sicherheit der verteilten Verwaltung von Rechten äußerst bedeutsam verbessert, wobei eine solche Sicherheit genauso hoch oder höher sein kann als die Sicherheit, die in zentralisierten Online-Handelsmodellen vorliegt.
- Kann zumindest einen Teil der Transaktionen innerhalb und/oder zwischen Teilnehmern der Wertkette (z. B. Organisationen, einzelnen Verbrauchern, virtuellen Gruppierungen) verwalten.
- Kann zumindest teilweise Erfüllungsbedingungen und/oder Konsequenzen von atomaren Transaktionen durch die Anwendung von Regeln und Steuermechanismen festlegen und/oder überwachen.
- Kann Ereignisse auf der Grundlage von Fehlerzuständen und/oder Transaktionsprofilanalysen (z. B. durch Verwendung einer Inferenzmaschine und/oder eines Expertensystems) leiten.
- Kann eine vertrauliche Zusammenarbeit von Sicherheits-, Routing-, Priorisierungs- und Verhandlungsprozessen bereitstellen, die es verschiedenen verteilten Parteien ermöglichen, über eine vertrauliche, vertrauenswürdige Schnittstelle effizient zusammenzuarbeiten.
- Bereitstellen einer Beglaubigung, Validierung, Zertifizierung und/oder gegebenenfalls Zustellung für sichere Dokumente und/oder Prozesskontrolle.
- Kann Schritte und/oder Übertragungswege zertifizieren, einschließlich das Zertifizieren des korrekten Weiterleitens für elektronische Daten über Telekommunikationsweichen von Transaktionsbehörden, die geeignet sind, bestimmte Daten zu zertifizieren und wobei Zertifikate zertifizieren, dass einem bestimmten Übertragungsweg gefolgt wurde oder nicht und/oder dass das Senden derartiger elektronischer Daten gemäß bestimmten vereinbarten Regeln und Steuermechanismen erfolgte, zum Beispiel, das Erwerben bestimmter Archivierungsdaten und/oder das Nicht-Überschreiten eines Budgets und/oder andere Begrenzungen für das Folgende: Anzahl von übertragenen Datencontainern in einer bestimmten Zeitspanne, Wert der darin enthaltenen (dadurch dargestellten) elektronischen Währung durch einen aktuellen Container und/oder durch Container über eine gewisse Zeitspanne hinweg, Menge an Geldmitteln die bei einem Kaufautrag ausgegeben werden kann, maßgebende Behörde für Bestellungen etc. werden ausgegeben um Anforderungen bezüglich des Empfangens eines derartigen maßgeblichen Zertifikats oder der Authentifizierung an einem Knoten, der eine derartige geführte Information empfängt, zu entsprechen.
- Verteilt dabei Funktionen der Transaktionsbehörde über ein Netzwerk oder ein anderes System (zum Beispiel ist jeder Knoten der Wertkette eines Verbrauchers und/oder jedes anderen Teilnehmern der Wertkette potenziell ein verteilter Usage-Clearingdienst, der wenigstens teilweise selbst als Transaktionsbehörde fungiert, und wobei besagter Teilnehmerknoten Benutzungsinformation direkt von einem oder mehreren Teilnehmern) übertragen kann sowie gemäß den Regeln und Steuermechanismen und weiteren VDE-Techniken wie in der Patentschrift von Ginter et al. beschrieben.
- Kann Schlichtungs-, Vermittlungs- und Verhandlungsdienste bereitstellen, dies können elektronische oder andere Dienste sein.

[0405] Fig. 55 zeigt eine bestimmte exemplarische Transaktionsbehörde **700** unter dem Gesichtspunkt all ihrer Funktionen. Transaktionsbehörde **700** stellt unter anderem eine sichere Audit-Einrichtung für das Aufrechterhalten des aktuellen Status einer globalen

Transaktion oder eines Prozesses, der auf Ereignisbenachrichtigungen von den Teilnehmern einer Transaktion basiert.

[0406] In dem spezifischen Beispiel kann die Zertifizierungsbehörde **700** die folgenden Funktionen ausführen:

- Erfassen von Ereignisanzeigen **730**,
- Validiertes Verwalten von Ereignisdatenbanken **732**,
- Erzeugung von Anforderungen **734**,
- Sicheres authentifiziertes Auditing **736**,
- Berichterstattung **738**,
- Benachrichtigungen erstellen **740**,
- Replikation **742**, und
- Propagierung **744**.

[0407] In diesem Beispiel empfängt Transaktionsbehörde **700** in Form von Ereignisanzeigen **748** Benachrichtigungen darüber, dass Ereignisse eingetreten sind, die in einem oder mehr sicheren elektronischen Containern **152** übermittelt werden können. Der Prozess für das Erfassen der Ereignisanzeigen **730** erfasst diese Ereignisanzeigen **748** und kann sie in einer validierten Ereignisdatenbank **732** speichern. Transaktionsbehörde **700** kann zusätzliche Benachrichtigungen **748** erzeugen, die auf validierten Ereignisdatenbanken **732** basieren, und kann auch Antworten **750** ausgeben, die den aktuellen Status einer Transaktion oder eines Prozesses als Antwort auf Anfragen **752** und/oder basierend auf anderen Anforderungen anzeigen. Zusätzlich kann die Transaktionsbehörde **700** Auditberichte **754** erzeugen und ausgeben, die den Fortschritt und den Status von Transaktionen oder Prozessen basierend auf den Inhalten ihrer validierten Ereignisdatenbanken **732**, wie von Prüffunktion **736** analysiert, anzeigen. Transaktionsbehörde **700** kann ebenfalls basierend auf ihrer Berichterstattungsfunktion **738** Berichte **756** ausgeben. Die validierte Ereignisdatenbank **732** kann eine verteilte Ereignisanzeigedatenbank sein, bei der der Replikationsprozess **742** und der Propagierungsprozess **744** verwendet werden, um die Datenbank dezentral zu pflegen und zu aktualisieren.

[0408] Eine weitere Hauptfunktion von Transaktionsbehörde **700** in diesem Beispiel ist das Ausgeben neuer oder geänderter Ereignisanforderungen **758**, die verwendet werden können, um einen Gesamtprozess oder eine Transaktion zu steuern oder zu beeinflussen. Transaktionsbehörde **700** kann Regelsatz **188**, Preise und Berechtigungen **188**, Ereignisflussanforderungen **760** und/oder Prozessroutinganforderungen **762** empfangen. Sowohl Ereignisflussanforderungen **760** als auch Prozessroutinganforderungen **762** können in einem oder mehr Regelsätzen festgelegt werden. Als Antwort auf diese Daten und die Inhalte der validierten Ereignisdatenbank **732** kann Transaktionsbehörde **700** den Anforderungsgenerierungsprozess **734** verwendet, um neue oder geänderte Ereignisanforderungen **758** zu erstellen. Transaktionsbehörde **700** kann auch neue oder geänderte Regelsätze **188"** und neue oder geänderte Preise und/oder Berechtigungen **188"'** erstellen. Transaktionsbehörde **700** kann Finanzaufstellungen als eine Eingabe für ihre sichere Auditfunktion **736** verwenden.

[0409] Fig. 56 zeigt einen exemplarischen Aufbau der Transaktionsbehörde **700**. In diesem Beispiel schließt Transaktionsbehörde **700** (die auf dem Aufbau des in Ginter et al. Fig. 12 und Fig. 13 gezeigten VDE-Rights Operating System („ROS") basieren kann) eine Einrichtung für sicheren Datenverkehr **770**, eine Datenbank und einen Transaktionsverarbeiter **772**, eine Prozesssteuerlogik **774**, Routingtabellen **776**, und eine lernfähige Datenbank für Regelsätze **778** (diese Funktionen können durch Verfahren an einem oder mehr Prüfpunkten durchgeführt werden), ein. Zusätzlich kann Transaktionsbehörde **700** auch einen Document Notarizer **780** einschließen, der einen Siegelgenerator **782**, einen Generator für einen digitalen Zeitstempel **784** und einen Fingerabdruck-/Wasserzeichengenerator **786** einschließt.

[0410] Die Einrichtung für sicheren Datenverkehr **770** ermöglicht es der Transaktionsbehörde **700**, auf sichere Art und Weise über elektronisches Netzwerk **150** (zum Beispiel über sichere elektronische Container **152**) zu kommunizieren. Datenbank und Transaktionsprozessor **772** führen die meisten der in Fig. 55 gezeigten Prozesse aus. Die lernfähige Datenbank von Regelsätzen **778** kann die Funktion der validierten Ereignisdatenbank ausführen. Routingtabellen **776** können als ein Teil der Anforderungsgenerierungsfunktion **734** verwendet werden, um die entsprechenden Nachrichten an entsprechende Einheiten zu richten.

[0411] Prozesssteuerlogik **774** kann eine Inferenzmaschine oder ein Expertensystem für die Verwendung bei der Verwaltung von Fehlerzuständen, die nicht vollständig von den Ereignisflussanforderungen **760** und/oder den Prozessroutinganforderungen **762** vorausgesehen oder festgelegt wurden, einschließen. Prozesssteuerungslogik **774** könnte auf der Grundlage von auf Regeln basierenden Prinzipien betrieben werden, Fuzzy Logik oder einer Kombination aus allen oder einigen davon – oder jedem anderen Verfahren der Prozesssteuerlogik. Prozesssteuerlogik **774** bestimmt das nächste Ereignis, das innerhalb der Gesamttransaktion oder des Prozesses auftreten soll.

[0412] Document Notarizer **780** kann verwendet werden, um die Erstellung von authentifizierten Dokumenten bereitzustellen, zum Beispiel um digitale Siegel und/oder stenographische Information an geschriebenen und/oder digitalen Dokumenten anzubringen.

[0413] Fig. 57 zeigt einen exemplarischen Prozess einer Transaktionsbehörde. In diesem vereinfachten Beispiel kann Transaktionsbehörde **700** eine Einheit innerhalb eines Unternehmens sein, die verwendet wird, um einen gesamten Güter-Auslieferungsprozess sicher zu prüfen und zu leiten. In diesem Beispiel gibt ein Verbraucher **95** eine Bestellung **788** über Güter aus. Diese Bestellung **788** wird von einer Abteilung für das Eingehen von Bestellungen **704** empfangen, die ein Bestellereignis **710** an Transaktionsbehörde **700** meldet. Als Antwort auf dieses Bestellereignis **710** kann Transaktionsbehörde **700** Regeln und/oder Anforderungen in Form von einem oder mehr Regelsätzen **188** ausgeben, die festlegen, wie die Abteilung für das Eingehen von Bestellungen **704** mit der Bestellung verfahren soll. Diese Regeln **188** können zum Beispiel eine Abfolge von Ketten und Verarbeitung festlegen, die auch die Aktivitäten einer Erfüllungsabteilung **709A**, eines Warenhauses **709B**, eines Transportunternehmens **726**, und einer Zahlungseinzugsabteilung **709C** leitet. Die Regeln **188**, die innerhalb von sicheren elektronischen Containern **152** von einer Abteilung zur nächsten weitergereicht werden können, legen so die Anforderungen und den Gesamtablauf des Transaktionsprozesses fest. Jede Abteilung kann dann die sicheren Regeln **188** an die nächste Abteilung weiterreichen, wobei das Weiterleiten durch die Regeln selbst und/oder durch die Transaktionsbehörde **700** organisiert wird. Jede Abteilung kann auch Ereignisanzeigen **748** ausgeben, die die Transaktionsbehörde **700** über den aktuellen Stand des globalen Prozesses in Kenntnis setzen. Transaktionsbehörde **700** kann dann diese Statusinformation zu Auditzwecken und/oder um zu ermöglichen, dass die Transaktionsbehörde den nächsten Schritt in dem Prozess einleitet, in ihrer sicheren validierten Ereignisdatenbank **732** speichern.

[0414] Transaktionsbehörde **700** kann zum Beispiel die in Fig. 17E-1 über Fig. 17E-4 gezeigten Interaktionsmodelle verwenden, um in die laufende Transaktion oder den Prozess Einfluss zu nehmen. Ein besonders nützliches Szenario für die Transaktionsbehörde ist das Verwalten eines Prozesses, der von mehreren Parteien ausgeführt wird, wie etwa Unternehmen, die im Rahmen eines Joint Venture oder um ein anderes gemeinsames Ziel zu erreichen, zusammenarbeiten. In diesem Geschäftsszenario können mehrere Unternehmen auf ein gemeinsames Ziel hinarbeiten, können aber selbst ihre eigenen internen Ziele haben, wie etwa zum Beispiel das Schützen ihrer eigenen vertraulichen, Handelsgeheimnissen unterliegenden Daten. Transaktionsbehörde **700** kann verwendet werden als ein unabhängiger Vermittler/Schlichter für das Koordinieren von Aktivitäten zwischen den mehreren Unternehmen, ohne dass eines der Unternehmen detaillierte Prozessinformation an jemand anderen als die Transaktionsbehörde **700** weitergeben muss.

[0415] Zum Beispiel kann Transaktionsbehörde **700** Regelsätze erzeugen, die Ereignisablauf- und/oder Prozessroutinganforderungen **758** und/oder Regelsätze **188** erzeugen, die in verschiedenen Kontexten verschiedene Bedeutungen haben. Als ein Beispiel kann ein von Transaktionsbehörde **700** ausgegebener Regelsatz bewirken, dass ein Unternehmen einen Schritt ausführt und ein anderes Unternehmen einen anderen Schritt ausführt – wobei keines der beiden Unternehmen jemals erfährt, welchen Schritt oder welche Abfolge von Schritten das jeweils andere Unternehmen ausführt. Somit kann Transaktionsbehörde **700** Regelsätze **188** aufstellen, die verwendet werden können, um lediglich eine teilweise Offenlegung der Aktivitäten verschiedener Akteure in Form von Einzelpersonen oder Unternehmen zu bewirken.

[0416] Fig. 58A und Fig. 58B zeigen exemplarische Schritte und Verfahren, die von Transaktionsbehörde **700** ausgeführt wurden, um eine „atomare Transaktion" durchzuführen. In diesem Beispiel hat Transaktionsbehörde **700** eine Rolle, die in gewisser Weise der des Trainers einer Fußballmannschaft vergleichbar ist. Durch das Annehmen des Leistungsspektrums und der Bedürfnisse jedes einzelnen „Spielers" und das Verbinden der Eigenschaften aller Spieler in einem globalen "Spielplan" kann die Transaktionsbehörde **700** eine beliebige Anzahl von Teilnehmern der Wertkette in eine globale „atomare Transaktion" einbinden.

[0417] In diesem Beispiel könnte jeder Teilnehmer der Wertkette **164(1)**, ... **164(N)** in einem von Transaktionsbehörde **700** geleiteten Prozess einen Regelsatz **188(1)**, ... **188(N)** beisteuern, der die Geschäftsbedingungen, Beschränkungen und Prozesse für die Transaktion jedes Teilnehmers festlegt und verwaltet (Fig. 58A und Fig. 58B, Block **750**). Diese individuellen Regelsätze **188(1)**, **188(N)** legen fest, wie jeder einzelne Teilnehmer seine jeweilige Rolle ausführt. Jeder Teilnehmer **164(1)** ... **164(N)** kennt seine Funktion in der Gesamttransaktion, aber es kann sein, dass er keine Kenntnis darüber hat, welche Funktionen andere haben oder genau weiß, wie sich ein "Team" aus anderen Teilnehmern zusammensetzt – und somit beschreiben diese individuellen Regelsätze **188(1)**, **188(N)** üblicherweise nur Sub-Transaktionen und es kann sein, dass sie die gesamte Transaktion betreffende Überlegungen nicht in Betracht ziehen.

[0418] Transaktionsbehörde **700** erhält auch einen weiteren Regelsatz **188X**, der festlegt, wie die Regelsätze der verschiedenen Teilnehmer miteinander in Gesamttransaktionsprozessen mit bestimmten Anforderungen und Einschränkungen (Fig. 58A und Fig. 58B, Block **752**). Diese die Gesamttransaktion betreffende Regelsatz **188Y** legt fest, wie Konflikte zwischen Sub-Transaktionen betreffenden Regelsätzen **188(1)**, **188(N)**, die von den einzelnen Teilneh-

mern bereitgestellt werden, gelöst werden (dies könnte zum Beispiel einen elektronischen Verhandlungsprozess **798** einschließen, wie in den **Fig.** 75A-76A der Patentschrift von Ginter et al. gezeigt). Die Transaktionsbehörde **700** verbindet die jeweiligen Regelsätze der einzelnen Teilnehmer – diese werden miteinander durch eine zusätzliche Logik verknüpft, um einen übergeordneten Regelsatz **188Y** für die Gesamttransaktion zu erstellen (Fig. 58A und Fig. 58B, Block **752**). Die Transaktionsbehörde speichert den resultierenden übergeordneten Regelsatz **188Y** in einem lokalen Speicher (Fig. 58B, Block **754**). Dieser übergeordnete Regelsatz regelt, wie die Transaktionsbehörde **700** Ereignisse verarbeitet, um eine „atomare Transaktion" durchzuführen.

[0419] Bei Empfangen eines eingehenden Ereignisses, das verarbeitet werden muss (Fig. 58B, Block **756**) kann Transaktionsbehörde **700** den übergeordneten Regelsatz der Gesamttransaktion **188Y** (Fig. 58B, Block **758**). Die Transaktionsbehörde **700** kann dann entsprechende wechselseitige Regelsätze entsprechend den Anteilen des übergeordneten Regelsatzes der Gesamttransaktion **188Y** an jeden Teilnehmer der Transaktion liefern – wodurch es jedem Teilnehmer ermöglicht wird, mit dem übergeordneten Regelsatz zu kommunizieren (Fig. 58B, Block **760**). Alternativ kann jeder Teilnehmer in diesem Beispiel – gleichzeitig, wenn er seinen Regelsatz **188(1)**, **188(N)** der Transaktionsbehörde **700** mitteilt – einen wechselseitigen Regelsatz beibehalten, der mit dem Regelsatz kommunizieren kann, den der Teilnehmer der Transaktionsbehörde **700** gesendet hat.

[0420] Transaktionsbehörde **700** kann dann damit beginnen, Ereignisse zu überwachen, die sie unter Verwendung des aktivierten übergeordneten Regelsatzes empfangen hat (Fig. 58B, Block **762**). Wenn das eingehende Ereignis keinen Fehlerzustand darstellt ("N"-Ausgang des Entscheidungsblocks **764** in Fig. 58B), dann legt Transaktionsbehörde **700** fest, ob das Ereignis anzeigt, dass die atomare Transaktion abgeschlossen ist (Fig. 58B, Block **765**). Wenn die atomare Transaktion nicht abgeschlossen ist („N"-Ausgang von Fig. 58B, Entscheidungsblock **765**), dann geht die Regel zurück zu Block **762**, um Ereignisse anzuzeigen. Wenn die atomare Transaktion abgeschlossen ist („Y"-Ausgang von Entscheidungsblock **765**), dann bestimmt die Transaktionsbehörde **700**, dass die Transaktion abgeschlossen ist (Fig. 58B, Block **774**).

[0421] Wenn das eingehende Ereignis einen Fehlerzustand darstellt ("Y"-Ausgang des Entscheidungsblocks **764** in Fig. 58B), dann verarbeitet Transaktionsbehörde **700** den Fehlerzustand in dem übergeordneten Regelsatz **188Y** (Fig. 58B, Block **766**). Wenn der Fehler nicht kritisch ist (Fig. 58B, Entscheidungsblock **767**, „N"-Ausgang), dann kehrt die Regel zu Block **762** zurück, um darauf zu erwarten, dass die nächste Ereignisanzeige ankommt.

[0422] Wenn der Fehler kritisch ist (Fig. 58B, Entscheidungsblock **767**, „Y"-Ausgang), kann Transaktionsbehörde **700** eine kritische Fehlerverarbeitungsroutine aufrufen (Fig. 58B, Block **768**). Die Verarbeitungsroutine **768** für kritische Fehler kann versuchen, den Fehler basierend auf den Regeln innerhalb des übergeordneten Regelsatzes und/oder auf einer Inferenzmaschine **774** oder anderen Prozesssteuerelektronik. Eine derartige Inferenzmaschine oder andere Prozesssteuerungselektronik **774** kann entsprechend dem Geschäftmodell der Gesamttransaktion programmiert werden, so dass sie genug Daten hat, um bei Fehlerzuständen geeignete Aktionen durchzuführen.

[0423] Das in Fig. 58B gezeigte Verfahren kann verschachtelt sein. Zum Beispiel kann die von einem „Teilnehmer" definierte Sub-Transaktion an sich eine atomare Transaktion sein, die auf den Einbringungen einer Anzahl von Teilnehmern basiert – von denen alle von derselben oder von verschiedenen Transaktionsbehörde(n) **700** verwaltet werden.

Commerce-Utility-System mit Sicherheits-Prüfpunkt

[0424] Ein Commerce-Utility-System **90** kann Unterstützungsfunktionen einschließen, die es ihm ermöglichen, als „Sicherheits-Prüfpunkt-System" **6000** zu wirken (siehe Fig. 58C), dass Sicherheits-, Archivierungs- und Nichtabweisungsdienste bereitstellt, die übertragene Information auf verschiedenen Wegen zertifizieren und/oder authentifizieren kann. Sicherheits-Prüfpunkt-System **6000** kann:

- eine verteilte, hocheffiziente und automatisierte Auditing und Archivierungsfunktion für elektronische Handelsinteraktionen bereitstellen, und
- die Sicherheitstiefe einer verteilten Sicherheitsumgebung wie etwa VDE und der Ebene des Distributed Commerce Utility erhöhen.

[0425] Somit kann Sicherheits-Prüfpunkt-System **6000** Sicherheits- und/oder Verwaltungsfunktionen ausführen. Diese Fähigkeit des Commerce Utility Systems weist die positiven Eigenschaften des zentralisierten Sicherheitsmodells (z. B. Fähigkeit, eine zentrale Behörde zu haben, die physikalisch den Verarbeitungsknoten kontrolliert) und weitet diese Eigenschaften zu einem verteilten "Benutzerraum"-Modell aus, mit dem maximale Effizienz und Flexibilität erreicht werden kann, sichere und verwaltbare Skalierbarkeit (eine Hauptschwäche des zentralisierten Systems und die verbesserte Sicherheit von mehreren unabhängigen, sicheren Umgebungen bereit. Die letztere Eigenschaft ist insbesondere geeignet für in höchstem Maße sensiblen Datenverkehr, bei dem zusätzliche Sicherheitsgarantien gewünscht werden. Diese Sicherheitsebenen werden möglich durch die erforderliche Teilnahme und Sicherheitsverarbeitung

von einer oder mehr unabhängigen geschützten Verarbeitungsumgebungen mit Sicherheitsprüfpunkt, was die Basis der verteilten Sicherheitsumgebung verstärkt.

[0426] Daten, die eines oder mehr Sicherheits-Prüfpunkt-Systeme **6000** passiert, kann zertifiziert und/oder authentifiziert werden, um einem Empfänger von Daten (z. B. einem Teilnehmer, der Daten in einem Container empfängt) zu gewährleisten, dass bestimmte Datenübertragungsfunktionen und/oder Sicherheitsschritte (Prozesse) vor dem Empfangen der Information geschehen sind. Diese Zertifizierung und/oder Authentifizierung kann zum Beispiel das Zertifizieren oder Authentifizieren von geeigneten Datenübertragungswegen durch erforderliche und/oder oder erlaubte geschützte Verarbeitungs-Sicherheit-Prüfpunkt-Systeme **6000** einschließen. Derartige Prüfpunkte können zum Beispiel über ein Telekommunikationsnetzwerk verteilt sein und „lokal" jeweils an der physikalischen oder logischen Adresse der VDE-Endnutzer-Knoten liegen.

[0427] Sicherheitsprüfpunktsysteme **6000** können Telekommunikationsschaltungen, die geeignet sind, bestimmte Informationen und Prozesse zu zertifizieren und/oder zu authentifizieren.

[0428] Zum Beispiel können von einem Sicherheitsprüfpunktsystem **6000** ausgegebene Zertifikate zertifizieren, dass ein benötigter Pfad verwendet wurde und dass ein benötigter Prüfpunkt einen übertragenen sicheren elektronischen Container untersucht hat, und/oder dass das Versenden eines derartigen Containers oder anderer elektronischer Daten gemäß bestimmter vorgegebener Regeln und Steuermechanismen durchgeführt wurde. Zum Beispiel kann ein derartiger Dienst unterstützen, zu gewährleisten und/oder zu zertifizieren und/oder zu authentifizieren, dass bestimmte Budgets, andere Einschränkungen und/oder Beschränkungen nicht überschritten werden und/oder bestimmte andere Anforderungen erfüllt sind.

[0429] Zum Beispiel kann ein Sicherheits-Prüfpunkt-System **600** dazu beitragen, das Erfüllen von Anforderungen sicher zu stellen (einschließlich des Nicht-Überschreitens von Einschränkungen oder anderen Beschränkungen) bezüglich: Anzahl von übertragenen Datencontainern in einer bestimmten Zeitspanne, Wert der darin enthaltenen (dargestellt durch) elektronische .

[0430] Währung durch einen aktuellen Container und/oder durch Container über eine gewisse Zeitspanne hinweg (sehr wichtig für das Verringern von unzulässigen elektronischen Zahlungsaktivitäten), Menge an Geldmitteln die bei einem Kaufauftrag ausgegeben werden kann, einschließlich der Tatsache, dass eine maßgebende Behörde für Bestellungen anwesend ist, und so weiter. Eine derartige Einschätzung der Anforderungen kann zum Beispiel in Bezug auf Datenverkehr über Container oder sonstige digitale Information erfolgen, wobei die Container von einem bestimmten logischen und/oder physikalischen Bereich, Knoten, Knotengruppe, Benutzer-Benutzer-Organisation und/oder anderen Gruppierungen von Benutzern übertragen wird, wobei der Bezug bestimmt wird durch das Herstellen eines Bezuges zu einem sicheren Knoten und/oder einzelnen Benutzern und/oder Organisationen und/oder Bereichsidentifizierungsdaten wie, zum Beispiel ein sicherer VDE-Container einen Weg durch besagte geeignete eine mehr Telekommunikationsweichen zurücklegt.

[0431] Diese Fähigkeiten der Übertragungsprüfpunkte eines Commerce Utility Systems können nützliche Sicherheitsmerkmale bereitstellen, indem sie zum Beispiel einen oder mehr „unabhängige" verteilte „Sicherheitsprüfpunkte" entlang eines Datenübetragungswegs bereitstellen, die im Wesentlichen die Sicherheit erhöht durch die Forderung nach dem Vorhandensein eines bestimmten Zertifikats und/oder einer Authentifizierung, die von einem derartigen Prüfpunkt sicher bereitgestellt wird und sicher verknüpft mit und/oder inkorporiert in dem Container ist durch ein Verfahren, das mittels des Prüfpunkts (oder einer Gruppe von Prüfpunkten) verwaltet wird. Dies kann durch den Empfängerknoten geprüft werden – und ein gültiges Zertifikat oder eine Authentifizierung können erforderlich sein, zum Beispiel gemäß den Regeln und Steuermechanismen, bevor ein derartiger Empfängerknoten wenigstens einen Teil des Inhalts von einer oder mehr Klassen von empfangenen Containern verarbeitet. Derartige Containerklassen können zum Beispiel Container von bestimmten Einzelpersonen und/oder Gruppen und/oder Containern und/oder Containerinhalten die ein bestimmtes Attribut oder mehrere bestimmte Attribute haben können.

[0432] Sicherheits-Prüfpunkt-Systeme **6000** können sicherheitstechnisch betrachtet „unabhängig" von den Endbenutzerknoten der Virtuellen Verteilungsumgebung sein. Derartige Knoten können zum Beispiel sicherheitstechnisch betrachtet unabhängig sein, weil sie eine Schlüsselverwaltung anwenden, um verschiedene sichere Ausführungsabteilungen innerhalb ihrer geschützten Verarbeitungsumgebungen zur Prüfpunktverwaltung unterhalten, sodass eine Sicherheitslücke in Endnutzerknoten nicht direkt die Sicherheit einer Prüfpunktoperation umfasst, und um sicherzustellen, dass eine mit einer sicheren Ausführungsabteilung in Beziehung stehende Lücke keine anderen derartigen Abteilungen umfasst.

[0433] Sicherheits-Prüfpunkt-Systeme **6000** können ebenfalls Auditdaten sammeln, einschließlich, zum Beispiel das Abrufen von Identitätsbezogenen Informationen von einer oder mehreren Personen,

die Container empfangen sollen, einer oder mehreren Klassen von Containerinformation, Prüfsummen und/oder weitere Informationen, die für zukünftige Validierung verwendet werden (z. B. Nicht-Abweisung) und/oder Archivieren von einigen oder sämtlichen Anteilen von Inhalten dieser Container. Einige dieser Daten können zumindest teilweise so verschlüsselt sein, dass eine oder mehr Anteile derartiger Daten nicht ohne die Kooperation von einem oder mehr Absendern von Containern entschlüsselt werden können, dem Empfänger, der den Container erhalten soll und/oder einer oder mehr aktuelle Empfänger des Containers und/oder einer Regierungsbehörde, wenn auf diese Daten zugegriffen werden soll.

[0434] Fig. 58C und Fig. 58D zeigen ein Beispiel für eine Anordnung eines Commerce Utility Systems **6000** mit „Sicherheitsprüfpunkt", das Sicherheit im Datenverkehr mittels eines Prüfpunkts, einer Funktion für die Nichtrückweisbarkeit und Archivierungsdiensten innerhalb des Kontexts eines Datenübertragungsnetzwerkes, das Benutzer **95(1)**, **95(2)**, **95(3)** miteinander verbindet, bereitstellt. In diesem Beispiel kann das Sicherheits-Prüfpunktsystem **6000** ein Teil der Datenübertragungs-Infrastruktur sein. Zum Beispiel können Sicherheits-Prüfpunktsysteme **6000** ein Teil von einer oder mehr Datenübertragungsweichen oder anderer Ausrüstung sein, die gestaltet wurde, um sichere elektronische Container **152** basierend zum Beispiel auf den Kopfdaten, die sie enthalten, zu identifizieren.

[0435] Sicherheitsprüfsysteme **6000** haben die sicherheitstechnische Eigenschaft, dass sie steuern können, ob ein sicherer Container **152**, der durch die Datenübertragungs-Infrastruktur übertragen wird, passieren darf oder nicht – sowie die Folgen des Leitens des Containers durch die Datenübertragungs-Infrastruktur. In einem Beispiel können Regeln, die mit einer geschützten Verarbeitungsumgebung eines Benutzers **95(1)** arbeiten, bestimmten Arten von Containern **152** erfordern (z. B. Container, die elektronische Währung transportieren), um Regeln **404** einzuschließen, die es erforderlich machen, dass diese durch Sicherheits-Prüfpunkt-Systeme **6000** (oder eine bestimmte Klasse von Sicherheits-Prüfpunkt-Systemen). Derartige Regeln **404** können verhindern, dass der Container **152** oder dessen Inhalt (z. B. die Währung, die er enthält) verwendet wird, außer im Falle, dass er durch das geeignete Sicherheits-Prüfpunkt-System **6000** geführt wird.

[0436] Zum Beispiel stelle man sich vor, dass der Benutzer **95(1)** einen sicheren Container **152** an Benutzer **95(2)** senden möchte. In diesem Beispiel überträgt der Benutzer **95(1)** den Container **152** an Benutzer **95(2)** über die Datenübertragungs-Infrastruktur. Diese Infrastruktur kann feststellen, dass die gesendete Information ein Container ist und kann den Container so leiten, dass er von dem Sicherheits-Prüfpunkt-System (System **6000(5)** zum Beispiel) abgefangen wird.

[0437] Sicherheits-Prüfpunkt-System **6000(5)** kann, nachdem es den Container **152** abgefangen hat, die in dem Container enthaltene Kontrollinformation untersuchen, um herauszufinden, ob die Bedingungen für das weitere Übertragen des Containers an den Benutzer **95(2)** erfüllt wurden. Sicherheits-Prüfpunkt-System **6000(5)** kann den Container an den Benutzer **95(2)** weiterleiten, jedoch nur dann, wenn die genannten Bedingungen erfüllt wurden – oder kann den Container verändern, um es Benutzer **95(2)** zu ermöglichen, den Container zu öffnen und ihn gemäß den Regeln **404** für diesen Container zu verwenden (die Regeln können zum Beispiel die Verwendung einschränken). Das Sicherheits-Prüfpunkt-System **6000** kann autorisiert sein, wenigstens einen Teil der Regeln des Containers **404** zu verändern – zum Beispiel um weitere Benutzungseinschränkungen hinzuzufügen.

[0438] Dieses Beispiel von Fig. 58C zeigt zwei „Netze" von Sicherheits-Prüfpunkt-Systemen **6000**. In diesem Beispiel stellen diese „Netze" Sammlungen von Sicherheits-Prüfpunkt-Systemen **6000** da, die jeweils folgendermaßen zertifiziert wurden (durch eine zertifizierende Behörde **500** zum Beispiel):

(1) ein Sicherheits-Prüfpunkt-System, und

(2) ein Mitglied der jeweiligen Klasse.

[0439] Somit stellt in diesem Beispiel „Netz 1" die Klasse der zertifizierten Sicherheits-Prüfpunkt-Systeme **6000(1)**-**6000(5)**, **6000(7)** dar, und Netz 2 stellt die Klasse der Sicherheits-Prüfpunkt-Systeme **6000(4)**-**6000(6)** dar. Als ein Beispiel können die Sicherheits-Prüfpunkt-Systeme **6000** von "Netz 1" derart zertifiziert sein, dass sie als fähig für das Verarbeiten von Containern mit elektronischem Geld **6004** gelten.

[0440] Eine der innerhalb der Steuerinformation festgelegten Anforderungen, die mit dem Container **152** assoziiert sind kann sein, dass er ein Sicherheits-Prüfpunkt-System von „Netz 2" passieren muss (z. B. System **6000(5)**) – zum Beispiel um bestimmte sichere Auditing-Funktionen wie etwa das vertrauenswürdige Verfolgen von elektronischem Geld. Ein Sicherheits-Prüfpunkt-System von „Netz 1" (z. B. System **6000(3)**) kann dem Container **152** die Weiterleitung an Benutzer **95(2)** verweigern, basierend auf diesen Regeln **404** – oder es kann verhindern, dass der Container **152** derart verändert wird, dass er durch Benutzer **95(2)** verwendet werden kann.

[0441] Als Beispiel stelle man sich vor, dass Benutzer **95(2)** wünscht, den Container **152** an einen anderen Benutzer **95(3)** weiterzuleiten. Die mit dem Container **152** assoziierten Regeln **404** können es in diesem speziellen Beispiel erfordern, dass der weitere

Datenverkehr des Containers **152** durch ein Sicherheits-Prüfpunkt-System **6000(7)** von "Netz 1" erfolgt. Diese Leitungsanforderung kann in den Regeln **404** vorliegen, die von dem Benutzer **95(1)** bereitgestellt wurden, oder sie kann über das Sicherheits-Prüfpunkt-System **6000(5)** oder die geschützte Verarbeitungsumgebung des Benutzers **95(2)** hinzugefügt werden.

[0442] In dem speziellen gezeigten Beispiel können die Regeln **404** zulassen, dass das Sicherheits-Prüfpunkt-System des „Netzes 1" **6000(7)** den Container **152** an Benutzer **95(3)** über eine weitere Strecke weiter leitet, welche kein Sicherheitsprüfpunktsystem **6000** einschließt (z. B. über eine andere Art von Commerce Utility System und/oder eine nicht sichere Datenübertragungsweiche.

[0443] Fig. 58D zeigt einen exemplarischen Prozess, der von einem exemplarischen Sicherheits-Prüfpunkt-System durchgeführt wurde. In diesem exemplarischen Verfahren empfängt das Sicherheits-Prüfpunkt-System **6000** einen Container **152** (Fig. 58D, Block **6002**) und beschreibt, ob die von den jeweils damit verknüpften Regeln **404** festgelegten Anforderungen erfüllt wurden oder nicht (Fig. 58D, Entscheidungsblock **6004**). Wenn die Bedingungen erfüllt worden sind, dann kann das Sicherheits-Prüfpunkt-System **6000** infolgedessen sogenannte "Bedingungen erfüllt"-Konsequenzen ausführen, z. B. das Verändern der Regeln **404** um die oben erwähnte Leitungsbedingung zu erfüllen (Fig. 58D, Block **6006**). Wenn die Bedingungen nicht erfüllt wurden (Fig. 58D, „N-Ausgang von Entscheidungsblock **6004**), dann kann das Sicherheits-Prüfpunkt-System sogenannte „Bedingungen nicht erfüllt"-Konsequenzen ausführen (Fig. 58D, Block **6008**).

[0444] Jeder Satz von Konsequenzen kann zum Beispiel eine bestimmte Art von sicherem Auditing einschließen. Wenn der Sicherheits-Prüfpunkt **6000** zum Beispiel einen Container **152** mit elektronischem Geld weiterreicht, dann kann der Sicherheits-Prüfpunkt **6000** einen oder mehr der folgenden Auditing-Daten aufzeichnen:

- Identität des Absenders,
- Senderknotenidentität,
- Empfängeridentität
- Empfängerknotenidentität,
- Zertifikat(e), auf dem(denen) das Geld basiert,
- weitere Sicherheits-Prüfpunkte **6000**, die das Geld passiert hat
- die Identität von vorangehenden Benutzern des Geldes,
- Datum, Uhrzeit und Ort der Übertragung,
- Datum, Uhrzeit und Ort des Empfangens,
- wie lange das Geld im Umlauf ist, und
- weitere sichere Auditing-Daten.

[0445] Wenn das Sicherheits-Prüfpunkt-System **6000** den Durchlass oder das Verändern eines Containers **152** verweigert, dann kann es einen Audit-Bericht erstellen, der verfügbare Daten für das Tracking einschließt, zum Beispiel folgende:

- Name des Absenders,
- Art des Fehlers,
- vorgesehener Empfänger, und
- weitere Information für das Tracking.

[0446] Es kann auch den Absender, den vorgesehenen Empfänger, eine Regierungsbehörde oder eine andere Behörde benachrichtigen. Es kann ferner zum Beispiel eine Gebühr für „fehlerhafte Weiterleitung" an den Sender richten.

[0447] Das Sicherheits-Prüfpunkt-System **6000** kann dann bestimmen, ob zusätzliche Datenübertragung notwendig ist (Fig. 58D, Entscheidungsblock **6010**). Wenn nicht kann der Vorgang abgeschlossen werden. Wenn zusätzliche Datenübertragung notwendig ist („Y"-Ausgang von Entscheidungsblock **6010**), dann kann das Sicherheits-Prüfpunkt-System **6000** den Container **152** an das nächste System weiterleiten (Fig. 58D, Block **6012**).

[0448] Das nächste System kann dann ein zusätzliches Sicherheits-Prüfpunkt-System **6000** sein, das eine zusätzliche Verarbeitung ausführt (Fig. 58D, Blöcke **6016**, **6004**, **6006**, **6008**).

BEISPIELE

Beispiel für ein Wertkette für den Vertrieb von elektronischem Inhalt

[0449] Fig. 59 zeigt, wie das exemplarische Distributed Commerce Utility **75** verwendet werden kann, um eine Wertkette für den Vertrieb von elektronischen Inhalten **162** zu unterstützen. In dem in Fig. 59 gezeigten Beispiel kann ein Autor **164** ein Werk mit einem gewissen Wert, wie etwa einen Roman, ein Fernsehprogramm, eine musikalische Komposition, oder ähnliches, schaffen. Der Autor stellt dieses Werk **166** für einen Herausgeber **168** zur Verfügung (zum Beispiel in elektronischer, digitaler Form).

[0450] Der Herausgeber kann sein eigenes Markenzeichen, seine Bekanntheit und seine Marketingstrategien verwenden, um das Werk einem Kunden **95** zu verkaufen. Der Herausgeber **168** kann das Werk **166** auch einem Inhaltsaggregator **170** zur Verfügung stellen – jemand, der Kunden Zugang zu einer großen Anzahl an Inhalten aus verschiedenen Quellen verschafft. Beispiele für Aggregatoren schließen zum Beispiel herkömmliche Online-Informationsdatenbankdienste und Internetseiten ein, auf denen Inhalte von vielen verschiedenen Seiten gelagert werden. Üblicherweise verwenden Benutzer einen Dienst eines Aggregatoren, indem sie Information bezüglich einer oder mehr von den Kunden definierten Begriffe

suchen. Ein Aggregator **170** kann dem Kunden **95**, der dann seine eigene Auswahl trifft, Suchwerkzeugzeuge zur Verfügung stellen.

[0451] Der Aggregator **170** könnte das Werk **172**, das einen Teil oder die Gesamtheit des Originalwerks **166** enthält, direkt an den Kunden **95** verkaufen. Aggregator **170** kann das Werk **172** auch an einen "Repackager" **174** vertreiben. Repackager **174** kann zum Beispiel Inhalt aus verschiedenen Quellen nehmen, der sich auf verwandte Themen bezieht und diese Inhalte zu Produkten mit verschiedenen Quellen kombinieren, wie etwa Multimedia-Kombinationen, Veröffentlichung von Newslettern oder Pakete über Themen von „aktuellem Interesse". In diesen Diensten trifft der Repackager die Auswahl des Inhalts und organisiert diesen anhand des von den Kunden bekundeten Interesses. Ein Kunde **95** kann einen elektronischen Newsletter abonnieren, der sich auf ein bestimmtes Thema bezieht, oder der Kunde kann dem Repackager **174** eine kurze Auflistung der Themen vorlegen, für die er sich interessiert. Der Repackager **174** wählt relevante Daten aus und leitet diese Daten an den Kunden weiter. Hierbei nimmt der Repackager die Auswahl für den Kunden vor.

[0452] Zum Beispiel kann der Repackager **174** der Herausgeber eines Newsletters sein kann einen Teil des Werks oder das gesamte Werk des Autors **166** in diesem Newsletter **176** erneut veröffentlichen. Repackager **174** könnte direkt Newsletter **176** an Verbraucher **95** verkaufen oder der Newsletter könnte noch andere zusätzliche Kanäle passieren. Repackager **174** könne eine Suchmaschine verwenden, die von Aggregator **170** zur Verfügung gestellt wird, um für Verbraucher **95** interessante Artikel zu finden und diese Artikel in einem elektronischen Newsletter zusammenstellen, der sowohl den Namen des Aggregators **170** als auch den des Repackagers **174** trägt und dann den Newsletter an den Verbraucher **95** senden.

[0453] Das Distributed Commerce Utility **75** kann die in Fig. 59 gezeigte Wertkette auf eine Vielzahl von Arten unterstützen. Zum Beispiel:

1. Zertifizierende Behörde **500** kann Zertifikate ausgeben, die jedem Teilnehmer der Wertkette ermöglichen, sich auszuweisen und zu beweisen, dass sie Mitglieder von einer oder mehr Klassen sind. Zum Beispiel könnten Autor **164** und/oder Herausgeber **168** festlegen, dass jeder zertifizierte Aggregator oder Repackager berechtigt ist, Auszüge oder Anthologien aus Werk **166** zu machen, solange eine angemessene Bezahlung erfolgt. Zertifizierende Behörde **500** könnte digitale Zertifikate **504** ausgeben, die dieses gewünschte Geschäftsziel unterstützen, wobei die Zertifikate zertifizieren, dass Aggregator **170** tatsächlich ein seriöser Aggregator ist und dass Repackager **174** tatsächlich ein seriöser Repackager ist. So lange Autor **164** und/oder Herausgeber **168** den Sicherheitsvorkehrungen des gesamten Systems und den von der zertifizierenden Behörde **500** ausgegebenen Zertifikaten **504** vertrauen, müssen sie nicht befürchten, dass das Werk **166** von irgendeiner anderen Person als denen, die sie als geeignet festgelegt haben exzerpiert oder eine Anthologie daraus erstellt wird .

[0454] In einem weiteren Beispiel könnte zertifizierende Behörde **500** ein Zertifikat **504** an Aggregator **170** oder einen weiteren Nutzer ausgeben. Zertifizierende Behörde **500** könnte dieses Zertifikat **504** an den Autor **164** oder den Herausgeber **168** ausgeben. Das Zertifikat **504** kann belegen, dass Autor **164** oder Herausgeber **168** damit einverstanden ist, dass Aggregator **170** oder ein anderer Benutzer autorisiert ist, bestimmte Berechtigungen zu verändern. Autor **164** oder Herausgeber **168** können spezielle Berechtigungen **404** haben, die nur unter der Bedingung verändert werden können, dass ein Zertifikat über einen „autorisierten Aggregatoren" vorliegt.

[0455] In einem weiteren Beispiel könnte zertifizierende Behörde **500** ein Zertifikat an einen oder mehr Klassen von Benutzern ausgeben, zum Beispiel für die Nutzung eines Inhalts und/oder besonderer Teile von Inhalten und/oder Änderung von Berechtigungen, die indem sie dies ermöglichen, auf eine bestimmte Art der Nutzung beschränkt sein können und/oder Änderungen durch das Anwenden von bestimmten VDE-Regeln und Steuermechanismen, die von dem Autor oder Herausgeber oder der zertifizierenden Behörde in Kraft gesetzt wurden (wie es durch Regeln und Steuermechanismen gestattet wird, die in Kraft sind).

2. Rechte- und Berechtigungs-Clearinghaus **400** kann in diesem speziellen Beispiel verwendet werden, das Werk **166** zu registrieren und geeignete Berechtigungen **404** auszustellen, die mit den von jedem Teilnehmer der Wertkette bereitgestellten Autorisierungen und Instruktionen übereinstimmen. Zum Beispiel kann der Autor **164** das Werk **166** mit Rechte- und Berechtigungs-Clearinghaus **400** registrieren und einen elektronischen Regelsatz **404** festlegen, der die Rechte jedes anderen Teilnehmers der Wertkette festlegt.

[0456] Zum Beispiel:

- Dieser Regelsatz **404** könnte, als ein Beispiel, festlegen, dass Herausgeber **168** eine unbegrenzte Anzahl von Kopien des Werks **166** vertreiben kann, solange der Herausgeber dem Autor **164** einen bestimmten Dollar-Betrag für jede verkaufte Kopie bezahlt.
- Der Regelsatz **404** kann es dem Herausgeber **168** erlauben, seine eigenen Zusatz-Regeln hinzuzufügen, die es dem Verbraucher **95** erlauben, das Werk **166** unbegrenzt oft zu lesen, jedoch verhindern, dass der Verbraucher das Werk kopiert

oder weiter verkauft.

• Obwohl der elektronische Regelsatz in einem elektronischen Container **152** zusammen mit dem Werk transportiert werden kann, kann er auch getrennt von diesem bereitgestellt werden. Zum Beispiel kann Rechte- und Berechtigungs-Clearinghaus **400** auf Anfrage einen mit Werk **166** verknüpften Regelsatz an jeden liefern, der einen Regelsatz anfordert.

[0457] Rechte- und Berechtigungs-Clearinghaus **400** kann verschiene Versionen des Regelsatzes **404** für verschiedene Benutzerklassen besitzen, so dass zum Beispiel Verbraucher **95** einen Regelsatz **404a** erhalten, Aggregatoren **170** könnten einen anderen Regelsatz **404b** erhalten, und Repackager **174** könnten wieder einen anderen, verschiedenen Regelsatz **404c** erhalten. Jedes dieser Regelsätze kann im Voraus von Autor **164** oder anderen Rechteinhabern bereitgestellt werden, und somit ein „im Voraus genehmigtes Berechtigungs"-System bereitstellen, das eine verbreitete Nutzung von Werk **166** äußerst effizient und doch in hohem Maße sicher macht, und ferner können Regelsätze mit verteilten VDE-Template-Anwendungen nahtlos zusammenarbeiten – eine oder mehr Template-Anwendungen können mit einem Regelsatz von Verteilern derartiger Regelsätze an Empfänger von Regelsätzen verteilt werden (oder können anders zugänglich gemacht werden). In einem speziellen, „Massenvertriebs-" Geschäftsmodell, kann Werk **166** so weit wie möglich vertrieben werden, und Rechte- und Berechtigungs-Clearinghaus **400** übernimmt die Funktion des Bereitstellens von Regelsätzen **404**, die es bestimmten Wertketten-Teilnehmern ermöglichen, das Werk unter bestimmten Bedingungen auf bestimmte Arten zu verwenden.

3. Usage-Clearinghaus **300** kann in diesem speziellen Beispiel die Wertkette durch das Sammeln von Benutzungsinformation von jedem Teilnehmer der Wertkette unterstützen. Das Usage-Clearinghaus **300** kann somit eine sichere Auditing-Funktion bereitstellen, indem es zum Beispiel Berichte erstellt, die verfolgen, wie viele Male das Werk **166** verwendet wurde und wie es verwendet wurde.

[0458] Als ein Beispiel kann Usage-Clearinghaus **300** Benutzungsinformation analysieren, um zu bestimmten, wie viele Verbraucher **95** das Werk gelesen haben. Usage-Clearinghaus **300** kann zum Beispiel Kaufinformationen verschiedenster Art für verschiedene Teilnehmer der Wertkette bereitstellen, die den Sicherheitsbedürfnissen und den akzeptierten geschäftlichen Rechten jeder Partei Rechnung tragen. Als ein Beispiel kann das Usage-Clearinghaus **300** Verbraucher **95** einen äußerst detaillierten Bericht über seinen oder ihren individuellen Gebrauch des Werks **166** abgeben, während Autor **164** oder Herausgeber **168** nur zusammenfassende Information in Form eines Berichts erhalten, die zum Beispiel den Namen des Verbrauchers, die Adresse oder andere direkte, Identitäts-bezogene Information nicht enthalten.

[0459] Als weiteres Beispiel könnten Berichte direkt von dem Repackager **174** zu dem Aggregator **170**, Herausgeber und Autor **164** fließen. Berichte können auf jedem logischen Weg, direkt oder über eine Anzahl von Parteien geschickt werden und können jede denkbare Zusammenstellung von Informationen für jede Partei enthalten, so wie es für die Wertkette annehmbar ist und können zum Beispiel zumindest teilweise durch VDE-Regeln und Steuermechanismen verstärkt werden.

4. Finanz-Clearinghaus **200** kann in diesem Beispiel sicheres Freigeben von finanziellen Details der Transaktion bereitstellen und so sicherstellen, dass geeignete Teilnehmer der Wertkette andere geeignete Teilnehmer der Wertkette für deren Aufwand entschuldigen. Als ein Beispiel kann Finanz-Clearinghaus **200** Zahlungen von Verbraucher **95** erhalten, die auf der Verwendung des Werks **166** durch den Verbraucher basieren, und Anteile der Bezahlung rechtmäßig auf Autor **164**, Herausgeber **168** und weitere geeignete Teilnehmer der Wertkette in einem automatisierten, effizienten Verafahren, das wenigstens teilweise durch VDE-Regeln und Steuermechanismen verwaltet wird, verteilen. Zum Beispiel kann Finanz-Clearinghaus **200** eine Schnittstelle zu anderen Banken oder Geldinstituten haben, um eine automatisierte Überweisung von Zahlungen vorzunehmen und/oder es kann beim Verwalten elektronischer Gelder mitwirken, die sich in der gezeigten Gesamt-Wertkette befinden. Finanz-Clearinghaus **200** kann auch dabei mitwirken, sicherzustellen, dass es selbst und die anderen Commerce Utility Systeme **90** entsprechend für die Verwaltungs- und Unterstützungsdienste, die sie bereitstellen, entschädigt werden, das heißt, zum Beispiel sichere VDE-Prozesse, die innerhalb von Commerce Utility Systemen **90** ausgeführt werden, können automatisch die Zahlung und derartiger Anbieter von Verwaltungs- und Unterstützungsdiensten sicherstellen.

5. Sichere Verzeichnisdienste **600** können in diesem Beispiel die exemplarische Wertkette durch das Vereinfachen des elektronischen Datenverkehrs zwischen Teilnehmern der Wertkette und oder zwischen Commerce Utility Systemen **90** unterstützen. Zum Beispiel kann sicherer Verzeichnisdienst **600** auf Anfrage elektronische Adressen- und Routingdaten bereitstellen, die es einem Teilnehmer der Wertkette ermöglichen, einen anderen auf elektronischem Wege zu kontaktieren. Als ein Beispiel sei angenommen, dass Verbraucher **95** die neueste Aktualisierung des Werks **166** erwerben will, jedoch feststellt, dass die elektronische Adresse des Herausgebers **168** sich geän-

dert hat. Verbraucher **95** kann den sicheren Verzeichnisdienst **600** auf elektronischem Wege kontaktieren, und dieser kann dann die aktuelle Adressinformation bereitstellen. Selbstverständlich kann der sichere Verzeichnisdienst in Anwendungen des kommerziellen Handels weitaus ausgefeiltere Dienste für die Identifizierung von gewünschten Parteien bereitstellen, wie etwa mehr-dimensionales Durchsuchen von Verzeichnisressourcen für das Identifizieren von Parteien basierend auf Klassenattributen. Sicherer Verzeichnisdienst **600** kann auch Dienste bereitstellen, die die Identifizierung von Inhalten ermöglichen, zum Beispiel basierend auf der Art des Inhalts und/oder Regeln und Steuermechanismen, die mit einem derartigen Inhalt verknüpft sind (Preisbildung, erlaubte Benutzungsparameter wie etwa Wiederverkaufsrechte etc.).

6. Transaktionsbehörde **700** könnte in diesem Beispiel verwendet werden, um Repackager **174** dabei zu unterstützen, Newsletter **176** zu erstellen. Zum Beispiel könnte Transaktionsbehörde **700** Unterstützung beim Automatisieren eines Prozesses bieten, bei dem eine Anzahl von verschiedenen Werken, die von einer Anzahl von verschiedenen Autoren allesamt für die Veröffentlichung in dem Newsletter aggregiert und exzerpiert wurden. Transaktionsbehörde **700** kann den jeweils aktuellen Status eines Gesamtprozesses mit mehreren Stufen sicher beibehalten und legt dabei fest, welche Schritte bereits ausgeführt wurden und welche Schritte noch ausgeführt werden müssen. Transaktionsbehörde **700** kann zum Beispiel auch zwischen verschiedenen Teilnehmern in einem derartigen Prozess mit mehreren Schritten schlichten und vermitteln und kann in einigen Fällen den Prozess beeinflussen oder steuern (zum Beispiel, durch das Herausgeben neuer Anweisungen oder Anforderungen, die auf Fehlerzuständen und anderem basieren.

Beispiel – Fertigungskette

[0460] Fig. 60 zeigt eine exemplarische Fertigungswertkette, die von dem Distributed Commerce Utility **75** unterstützt wird. In diesem speziellen Beispiel richtet ein Verbraucher **95** einen Auftrag an einen Hersteller **180** und erhält eine Auftragsbestätigung. Der Hersteller kann Teile bestellen und bezieht diese von einer Anzahl verschiedener Zulieferer **182(1) 182(N)**. Zulieferer **181(1)**-**182(N)** können wiederum zusätzliche Teile oder Montageteile von weiteren Zuliefern **182(a1)** bestellen. Eine Bank **184** kann den Zulieferern **182** Geldmittel zur Verfügung stellen, basierend auf Nachweisen, dass tatsächliche eine Bestellung eingegangen ist und Garantien dafür, dass der Hersteller die Vorauszahlungen zurückzahlen wird. Ein Transport/Lagerunternehmen 186 kann für den Transport und die Lagerung für zugelieferte Produkte und/oder Endprodukte sorgen.

[0461] In dieser Wertkette können zertifizierende Behörde **500** und Transaktionsbehörde **700** mit sicherer Weiterleitung elektronischer Bestellungen, Bestätigungen, Geschäftsbedingungen und Verträgen unterstützen und können auch dazu beitragen, dass sichergestellt ist, dass jeder Teilnehmer der Wertkette das gewünschte Maß an Vertrauenswürdigkeit beim Austauschen von notwendigen Daten mit Teilnehmern der Wertkette aufbringt. Usage-Clearinghaus **300** kann das sichere Auditing des Gesamtprozesses, das Verfolgen von tatsächlichen und elektronischen Paketen zwischen den Teilnehmern der Wertkette und weiteren Benutzungs-relevanten Vorgängen unterstützend mitwirken. Finanz-Clearinghaus **200** kann die finanziellen Vereinbarungen zwischen den Teilnehmern der Wertkette verwalten, zum Beispiel unterstützende Koordination zwischen dem Bereich des elektronischen Netzwerks **150** und einem Bankbereich, der mit Dokumenten in Papierform arbeitet oder einem anderen Bankbereich, bereitstellen. Transaktionsbehörde **700** kann den Gesamtfortschritt von Transaktionen zwischen Teilnehmern der Wertkette sicher überwachen und gegebenenfalls periodische Statusberichte an jeden Teilnehmer der Wertkette bereitstellen. Zusätzlich kann Transaktionsbehörde **700** unterstützend mitwirken beim Regeln der globalen Transaktionen, um sicherzustellen, dass alle Schritte durchgeführt und alle Forderungen erfüllt wurden. Sichere Verzeichnisdienste **600** können unterstützend tätig sein beim elektronischen Routen von Daten zwischen den verschiedenen Teilnehmern der Wertkette. Selbstverständlich kann die VDE-Verarbeitungs- und Steuerungskette, wie sie vorangehend für die vorliegenden Erfindungen dargelegt ist und für die gesamte Anmeldung gültig sein soll, und weitere Eigenschaften, einschließlich von Regeln und Steuermechanismen und sicheren Datenübertragungstechniken bevorzugt als eine Grundlage für die obigen Aktivitäten verwendet werden.

Beispiele dafür, wie Commerce Utility Systeme sich gegenseitig unterstützen können

[0462] Die oben beschriebenen Fig. 16A-Fig. 16E zeigen, wie verschiedene Commerce Utility Systeme **90** einander unterstützen können. Genauer gesagt zeigt Fig. 16A, dass ein Finanz-Clearinghaus **200** Dienste für eines oder mehr Commerce Utility Systeme **90** bereitstellen kann, einschließlich, zum Beispiel das Usage-Clearinghaus **300**, das Rechte- und Berechtigungs-Clearinghaus **400**, die zertifizierende Behörde **500**, die sicheren Verzeichnisdienste **600**, die Transaktionsbehörde **700** und ein anderes Finanz-Clearinghaus **200'**. Unter derartigen Umständen stellen die vielen Commerce Utility Systeme sowohl ein virtuelles Clearinghaus als auch ein höher geordnetes Commerce Utility System dar.

[0463] Auf jeder Ebene kann das Finanz-Clearing-

haus an die Unterstützungsdienste zu zahlende Beträge einholen und diese Gelder auf das Konto eines Anbieters einzahlen, wobei wenigstens eine Zahlungsmethode angewendet wird. Das Finanz-Clearinghaus **200** kann auch VDE-Audit-Aufzeichnungen, welche die Herkunft und die Höhe der Geldmittel sowie das Konto des Anbieters, auf das die Gelder von dem Finanz-Clearinghaus eingezahlt wurden bestätigen. Das Finanz-Clearinghaus **200** kann einen oder mehr andere Unterstützendienste dabei unterstützen, Anbieterkonten einzurichten und den einen oder mehr Unterstützungsdiensten die Kontonummer und/oder Kontonummern und Geschäftsbedingungen, die sie anwenden können, mitteilen. Sowohl die Anfrage nach unterstützenden Diensten an das Finanz-Clearinghaus **200** und dessen Antworten an den anfordernden Unterstützungsdienst können in sicheren VDE-Containern übertragen werden (wie weiter oben bereits erwähnt), um deren hohe Sicherheit, Vertraulichkeit, flexible Kontrollstruktur und Vertrauenswürdigkeit zunutzen und können an jeder Stelle von der einer oder mehr geschützten VDE-Verarbeitungsumgebungen verarbeitet werden. Finanz- und Kontendaten können in Form von VDE-Regelsätzen bereitgestellt werden und/oder in VDE-Regelsätzen inkorporiert werden durch das Finanz-Clearinghaus **200** und/oder durch einen oder mehr Unterstützungsdienste. Finanz-Clearinghaus **200** kann sich auch gegenseitig mit Diensten unterstützen, um mehr Betriebs- und Verwaltungseffizienz zu fördern. Zum Beispiel kann ein Finanz-Clearinghaus **200** Dienste an ihre jeweiligen Gegenstücke in anderen Ländern oder anderen Regionen bereitstellen. In einem weiteren Beispiel kann ein Finanz-Clearinghaus 200 einem weiteren Finanz-Clearinghaus **200** Zugang zu einer oder mehr Bezahlungsarten verschaffen, die nicht direkt von dem zweiten Finanz-Clearinghaus **200** unterstützt werden.

[0464] Fig. 16B zeigt, dass das Usage-Clearinghaus **300** auch Dienste an andere Commerce Utility Systeme **90** bereitstellen kann. In einem Beispiel kann das Usage-Clearinghaus **300** Rohdaten, aggregierte Daten, wenigstens teilweise abgeleitete Informationen und/oder Berichte an andere Unterstützungssysteme für elektronischen Handel wie etwa Finanz-Clearinghäuser **200**, Rechte- und Berechtigungs-Clearinghäuser **400**, zertifizierende Behörden **500**, sichere Verzeichnisdienste **600**, Transaktionsbehörden **700** und weitere Usage-Clearinghäuser **300'** bereitstellen. Diese weiteren Infrastrukturdienste können diese Daten als Beleg für bestimmte Transaktionen und deren Details, für Marktsuche bezüglich ihrer eigenen Dienste und/oder um diese Daten weiter zu verkaufen, möglicherweise in Verbindung mir ihren eigenen Benutzungsdaten verwenden. Als ein Beispiel könnte Rechte- und Berechtigungs-Clearinghaus **400** Berichte an einen Herausgeber verkaufen, die eine Zusammenstellung ihrer eigenen Daten enthalten, und die das Finanz-Clearinghaus **200** und das Usage-Clearinghaus **300** plus sichere Verzeichnisdienste **600** und zertifizierende Behörde **500** bilden. Insbesondere kann ein Bericht eine Liste von bei dem Rechte- und Berechtigungs-Clearinghaus **400** von einem bestimmten Herausgeber registrierten Objekten enthalten, die Anzahl der Anforderungen des Rechte- und Berechtigungs-Clearinghauses für aktualisierte und zusätzliche Rechte und Berechtigungen, zusammenfassende Berichte über Einkommen des Finanz-Clearinghauses für jedes digitale Eigentum, die Anzahl der Zertifikate der zertifizierenden Behörde **500** im Auftrag des Herausgebers, die anzeigen, dass der Benutzer zertifiziert wurde und die digitalen Werke des Herausgebers rechtmäßig abonniert hat, und die Anzahl der Anforderungen an den sicheren Verzeichnisdienst **600**, der Daten bezüglich der Netzwerkadressen der Online-Webserver des Herausgebers sucht. In jedem Fall hat ein Unterstützungsdienst die Daten für das Rechte- und Berechtigungs-Clearinghaus zur Einführung in diesen Bericht dem Herausgeber zur Verfügung gestellt.

Beispiel – Das Distributed Commerce Utility **75** kann das Lizenzieren von digitalem Eigentum und/oder Verleihtransaktionen unterstützen

[0465] Das Distributed Commerce Utility **75** stellt signifikante Vertrauenswürdigkeit, Sicherheit, Komfort und Effizienzen für Vorgänge bereit, in denen Kunden für digitale Information bezahlen. Zudem können Ersteller und Verteiler von Information den Preis für diese Information und jedes digitale Eigentum in jedem digitalen Format auf verschiedene Arten festsetzen und auf verschiedene Arten in verschiedenen Märkten.

[0466] Fig. 61 zeigt ein Beispiel für eine Anordnung eines Dienstes für das Übermitteln von Daten **1000** indem ein Informationsanbieter **168** elektronischen Inhalt für Einkauf, Verleih und/oder Vergeben von Lizenzen bereitstellt. In diesem Beispiel verteilt ein Informationsdienstunternehmen **168** Information **166** an verschiedene globale Märkte einschließlich Einzelpersonen. Ihr Marktbereich schließt Geschäftspersonen, Nutzer von Heimbüros und den Marktbereich der Kleinbüros ein, sowie mittlere und große Unternehmen und Verbraucher zuhause. Zum Beispiel kann Anbieter **168** Inhalt **166** in elektronischer Form an einen Heimverbraucher **95(1)** liefern, eine Geschäftsperson wie etwa einen Anwalt **95(2)** und an ein Unternehmen oder eine andere Organisation **95(3)**. In einem Beispiel:

- kauft ein Privatkunde **95(1)** unter Abonnementpreisbedingungen drei Artikel **166(1)** einer Online-Enzyklopädie.
- kauft ein Anwalt **95(2)** drei Kapitel **166(2)** einer Abhandlung über Patentrecht und
- zwei Produktmarketing-Manager eines großen Unternehmens **95(3)** erhalten einen Forschungs-

bericht über den Markt des geistigen Eigentums **166(3)**.

[0467] Vor Informationsübergabetransaktionen können der Verbraucher **95(1)**, die Geschäftsperson **95(2)** und das Unternehmen **95(3)** einen sicheren Verzeichnisdienst **600** verwenden, um die Netzwerkadresse des Anbieters der Information **168** bereitzustellen so wie dabei mitzuhelfen, den Inhalt, mit dem sie arbeiten möchten zu identifizieren. Anschließend könnten diese Parteien **95** eine elektronische Nachricht an Anbieter **168** senden und die jeweilige Information, die sie erhalten möchten. Anbieter **168** kann diese Information **166** im Inneren des sicheren elektronischen VDE-Containers **152** zusammen mit verknüpften Regeln und Steuermechanismen anfordern, die die Festlegung von Preisen und die Berechtigungen steuern. Jede der Parteien **95** hat ein elektronisches Gerät **100**, das eine geschützte Verarbeitungsumgebung **154** einschließt, die diese Regeln **188** verstärkt.

[0468] Der Anbieter **168** kann für verschiedene Märkte verschieden Preise festlegen. Zum Beispiel:

- Geschäftspersonen **95(2)** und SOHO (small office/home office, kleines Büro oder Heimbüro) zahlen Gebühren für die Transaktion;
- große Unternehmen **95(3)** bezahlen eine Mischung aus Abonnierungs- und Transaktionsgebühren (z. B. kann Unternehmen **95(3)** $ 10 pro Ausdruck oder Auszug aus einem größeren Bericht bezahlen und kann auch eine Abonnierungsgebühr bezahlen), und
- Privatverbraucher **95(1)** bezahlen eine niedrige Abonnierungsgebühr.

[0469] Im jedem Fall sind gegebenenfalls lokale, bundesstaatliche und/oder gesamtstaatliche Umsatzsteuern in dem Verkaufspreis enthalten. Zahlungsarten können innerhalb elektronischer Regelsätze **188** bereitgestellt werden, die in elektronischen Containern **152** mit/und oder unabhängig von dem assoziierten Inhalt **166** geliefert werden könne (zum Beispiel wie in Ginter et al. bereitgestellt).

[0470] Ein Finanz-Clearinghaus **200** stellt sicher, dass Anbieter **168** Bezahlung über jegliche erlaubte Zahlungsmethode erhält. Der Dienst für das Liefern der Daten **168** akzeptiert eine große Bandbreite von Zahlungsmethoden. Einige Zahlungsarten sind in einigen Märkten beliebter als in anderen. Zum Beispiel:

- in dem Markt der Geschäftspersonen, SOHO und Verbraucher, sind Gutschrift (MasterCard und Visa) und Lastschrift (American Express) beliebte Zahlungsarten.
- Verbraucher **95(1)** mögen Kreditkarten ebenfalls und verwenden zunehmend Lastschriftkarten.
- Große Unternehmen **95(3)** verwenden ebenfalls Kreditkarten und Lastschriftkarten, Bezahlung über automatisierte Clearinghäuser (ACHs, automated Clearinghouses) und Abrechnung und Bezahlung über sichere herkömmliche und VDE-Electronic Data Interchange (EDI)-Transaktionen, die beispielsweise auf X.12-Protokollen basieren.

[0471] Ein Finanz-Clearinghaus **200** gestaltet die Bezahlung auf verschiedene Arten wirksamer. Zum Beispiel beliefert Finanz-Clearinghaus **200** Anbieter **168** mit einer bequemen, "One Stop Shopping"-Benutzeroberfläche mit den mehreren Zahlungsarten und verfolgt die wenigstens eine mit einem bestimmten Anbieter assoziierte Kontonummer.

[0472] In diesem speziellen Beispiel kann eine zertifizierende Behörde **500** digitale Zertifikate an jeden Verbraucher **95** liefern, die die eine oder mehr Klasse(n) eines Verbrauchers festlegen. Zum Beispiel kann zertifizierende Behörde **500** folgendes ausstellen:

- eines oder mehr Zertifikate **504(1)**, die die Tatsache nachweisen, dass Verbraucher **95(1)** als Privatperson Abonnent von Informationsdienst **1000** ist und ferner attestiert, dass der Verbraucher ein eingeschriebener Student an einer Hochschule ist und seinen Wohnsitz (für die mit der Transaktion verbundene Besteuerung) in Kalifornien hat.
- ein Zertifikat **504(2)** weist nach, dass Geschäftsperson **95(2)** für Gerichte des Staates Kalifornien zugelassener Anwalt ist, und
- eines oder mehr Zertifikate **504(3)** weisen nach, dass Unternehmen **95(3)** eine rechtmäßig eingetragene Kapitalgesellschaft ist und eine gewisse Kreditwürdigkeit besitzt.

[0473] Regelsätze **188** können die verschiedenen Zahlungsarten basierend je nach Vorhandensein eines geeigneten digitalen Zertifikats **504** aktivieren.

[0474] Zum Beispiel autorisiert Regelsatz **188(1)**, der an das elektronische Gerät **100(1)** des Verbrauchers gesendet wird Verbraucher **95(1)** dazu, jeden dieser drei Artikel **166(1)** zu verwenden. Regelsatz **188(1)** kann zum Beispiel eine Bedingung enthalten, die vorschreibt, dass der Verbraucher **95(1)** ein Zertifikat **504(1)** von einer unabhängigen zertifizierenden Behörde **500** (oder von einem Verteiler von Daten oder anderen Partei, die die Funktion einer zertifizierenden Behörde ausführt unter Autorisierung durch eine übergeordnete zertifizierende Behörde) haben muss, das attestiert, dass der Verbraucher **95(1)** ein noch nicht abgelaufenes Abonnement für die Online-Enzyklopädie hat. Dieses Zertifikat **504(1)** kann zum Beispiel in Verbindung mit anderen von der zertifizierenden Behörde **500** ausgestellten Zertifikaten (z. B. von der US-Regierung oder einer anderen Aufsichtsbehörde betrieben oder autorisiert) und kann nachweisen, dass der Verbraucher **95(1)** ein US-Bürger ist, US-Bürger ist und seinen eingetragenen Wohnsitz im Staate Kalifornien hat.

Der Einzelverbraucher

[0475] Der Verbraucher **95(1)** bezahlt den Anbieter von Information **168** für das Abonnement über eine an das Finanz-Clearinghaus **200** übermittelte Transaktion in einem elektronischen VDE-Container **152**. Die Zahlungstransaktion kann zum Beispiel einschließen, dass das benutzerseitige Gerät **100** einen elektronischen Container **152(7)** an das Finanz-Clearinghaus **200** sendet, einschließlich der Regeln und Steuermechanismen **188(4)** und der Audit-Aufzeichnungen **302(1)**. Die Audit-Aufzeichnungen **302(1)** können zum Beispiel folgendes anzeigen:

- wer bezahlt werden soll
- den Überweisungsbetrag
- die jeweilige Zahlungsart (zum Beispiel per VISA-Karte)
- die VISA-Kartennummer des Abonnenten und das Datum, an dem diese ungültig wird,
- eine Kennnummer für das Abonnement, und
- die Kontonummer des Anbieters, auf das die Zahlung gutgeschrieben werden soll.

[0476] Der sichere Container **152(7)** kann auch Regeln und Steuermechanismen **188(4)** enthalten, die angeben, dass Umsatzsteuern der jeweiligen Gemeinde, des Staates Kalifornien und der Vereinigten Staaten eingezogen werden können. Das Finanz-Clearinghaus **200** zieht die vorgeschriebenen Umsatzsteuern ein und überweist die Gelder an die jeweiligen Konten, zum Beispiel werden bestimmte Gelder an das entsprechende Konto der Steuereinzugsbehörde des Staates Kalifornien **1002** überwiesen.

[0477] Als Gegenwert für die Zahlung kann der Abo-Kundin **95(1)** von der zertifizierenden Behörde **500** ein Zertifikat **504(1)** erhalten, das angibt, dass sie tatsächlich eine Abonnentin ist sowie das Ablaufdatum des aktuellen Abonnements.

Die Geschäftsperson

[0478] Der Anwalt **95(2)** in diesem Beispiel kann seinen Sitz im vereinigten Königreich haben. Er erwirbt die drei Kapitel **166(2)** einer Abhandlung über Patente unter Verwendung einer Master-Card, bezahlt jedoch in Pfund Sterling anstatt in Dollar. Um die Einkaufstransaktion durchzuführen, kann der Anwalt **95(2)** zunächst eine Vor-Autorisierung von dem Finanz-Clearinghaus **200** bekommen, die ihn zu monatlichen Einkäufen im Wert von bis zu $500 US (oder einen äquivalenten Betrag in Pfund) berechtigen. Die Vor-Autorisierung kann von dem Finanz-Clearinghaus **200** an das benutzerseitige Gerät **100(2)** gesendet werden in Form einer Budgetprüfung **188(5)** in einem sicheren Container **152(8)**. Die geschützte Verarbeitungsumgebung **154(2)** innerhalb des Geräts des Anwalts **100(3)** kann den Container **152(8)** öffnen, den Budgetbericht **188(5)** authentifizieren und die Regel innerhalb einer assoziierten sicheren Datenbank, die von PPE **154(2)** unterhalten wird, speichern.

[0479] Bei Erhalt und Öffnen jedes der drei Kapitel **166(1)** kann die geschützte Verarbeitungsumgebung **154(2)** eine assoziierten Audit-Aufzeichnung erstellen und in dem Budgetbericht den Einkaufsbetrag von dem verfügbaren Kreditrahmen abziehen. Am Monatsende, wenn der vorautorisierte Kredit von $500 erschöpft ist, kann die PPE des Anwalt **154(2)** an das Finanz-Clearinghaus **200** einen sicheren Container **152(9)** mit Audit-Aufzeichnungen **302(2)** senden, die sämtliche Einkäufe, deren Beträge und die Anbieterkonten oder Konten, auf die gutgeschrieben werden soll, anzeigen, wobei dies eine wirksame Automatisierung von Clearing-Prozessen unterstützt. Das Finanz-Clearinghaus **200** kann den sicheren Container **152(9)** öffnen, das Kreditkartenkonto des Anwalts belasten und den jeweiligen Anbieterkonten den fälligen Betrag zu überweisen.

Das Unternehmen

[0480] Vor der Übertragung von Inhalten, sendet ein verteiltes, Kapital-Finanz-Clearinghaus **200A** innerhalb des Unternehmens **95(3)** unter der Aufsicht des Finanz-Clearinghauses **200** jedem der Manager **95(3)A**, **95(3)B** einen sicheren Container **152**, einen Budgetbericht **188**, der ihr aktuell bewilligtes monatliches Informations- und Marktforschungsbudget angibt. Eine verteilte zertifizierende Behörde in Form eines Unternehmens **500A** (die sich in derselben Vertrauenswürdigkeitshierarchie wie die zertifizierende Behörde **500** in diesem Beispiel befindet), kann auch digitale Zertifikate **504** (nicht gezeigt) für Angestellte dieses Unternehmens ausstellen.

[0481] In diesem Beispiel druckt jeder Produktmanager **95(3)A**, **95(3)B** ausgewählte Bereiche des Berichts und des Budgets auf seinem oder ihren lokalen Gerät **100**, wofür $ 10 pro gedruckte Seite berechnet werden. Die geschützte Verarbeitungsumgebung **154(3)** innerhalb des lokalen elektronischen Geräts **100(3)** kann diesen Vorgang sicher ausführen und ihn auf Regeln **188(3)** abstimmten, die korrekte digitale Zertifikate **504(3)** verlangen, die von einer zertifizierenden Behörde **500** und/oder der verteilten zertifizierenden Behörde des Unternehmens **500A** ausgestellt wurden.

[0482] Gemäß den Regeln **188(3)**, die von dem Informationsanbieter geliefert werden, beispielsweise zum Monatsende oder wenn das Budget für diesen Monat erschöpft ist, sendet das Gerät des Unternehmens **100(3)** an das interne Finanz-Clearinghaus des Unternehmens **200A** Audit-Aufzeichnungen (nicht gezeigt), die jeden Einkauf, der während des Berichterstattungszeitraums getätigt wurde sowie den Beträgen und den Kontonummern der Anbieter für der-

artige Käufe. Das verteilte lokale Finanz-Clearinghaus **200A** des Unternehmens aggregiert die Summen in den Audit-Aufzeichnungen und sendet wenigstens einen Prüfbericht **302(3)** in einem sicheren Container an das externe Finanz-Clearinghaus **200** um die Zahlung des Gesamtbetrages, der dem Anbieter der Marktforschungsberichte geschuldet wird, über ein automatisiertes Clearinghaus (ACH) zu autorisieren. In dem sicheren Container **152(11)** (z. B. als Teil einer Audit-Aufzeichnung **302(3)**) finden sich die Kontonummer des Unternehmens **95(3)**, von dem die Gelder abgebucht werden sollen sowie die Kontonummer des Marktforschungsunternehmens, das den Bericht ausgegeben hat, für den die Gelder bezahlt werden sollen. Das Finanzclearinghaus **200** schließt den Zahlungsvorgang durch das ACH ab und sendet einen sicheren VDE-Container (der wenigstens eine Audit-Aufzeichnungen bereitstellt) zurück an das interne Finanz-Clearinghaus des Unternehmens **200A** als Bestätigung. Verteiltes Clearinghaus **200A** kann wiederum wenigstens eine bestätigende Audit-Aufzeichnung an jeden Produktmanager **95(3)A**, **95(3)B** unter Verwendung eines sicheren Containers (nicht gezeigt).

Beispiel: Das Distributed Commerce Utility **75** kann Transaktionen, in denen ein Verbraucher einen materiellen Gegenstand kauft und diesen bezahlt, unterstützen.

[0483] Ein bedeutsamer Anteil des elektronischen Handels wird Verkaufs-, Einkaufs- und Verteilungsmanagement und/oder Bezahlung für immaterielle Güter nach sich ziehen. Handel mit materiellen Gütern hat in vielen Punkten die gleichen Anforderungen an Sicherheit, Vertrauenswürdigkeit und Effizienz wie Handel mit immateriellen Gütern (z. B. digitalen Daten). Damit der Computer ein richtiges Handelsgerät wird, ist eine verteilte, sichere, vertrauenswürdige Softwareebene für das Verwalten von Rechten/Ereignissen notwendig (z. B. Rights Operating System oder Middleware), wie etwa die in der Ginter et al. Patentschrift beschriebene virtuelle Verteilungsumgebung. Somit kann, auch wenn materielle anstatt digitaler Güter im sicheren elektronischen Handel gehandelt werden, das Distributed Commerce Utility **75** eine wichtige Rolle spielen.

[0484] Fig. 62 zeigt ein Beispiel für ein System für den Einkauf von materiellen Gütern und ein Bezahlungssystem **1010**. In dem in Fig. 62 gezeigten Beispiel stelle man sich vor, dass ein gut bekannter Anbieter von Kleidung und bestimmten damit in Verbindung stehenden Haushaltsgütern, zum Beispiel L.L. Bean oder Land's End, seine Waren über ein digitales Netzwerk wie etwa das Internet/World Wide Web anbietet. In diesem Beispiel erstellt das Unternehmen folgendes:

- einen Internet-Katalogserver **1012**, um dem Verbraucher **95** eine Kollektion anzubieten,
- einen Internet-Erfüllungsserver **1014**, der eine Schnittstelle zu der Erfüllungsfunktion ist, und
- einen dritten Webserver **1016** als ein sicheres Finanzclearinghaus **200** und als eine Schnittstelle zu einigen Zahlungsarten (z. B. MasterCard („MC), VISA und American Express („AMEX")).

[0485] In diesem Beispiel tut das Unternehmen auch folgendes:

- registriert die Dienste mit dem Anbieter des sicheren Verzeichnisdienstes **600**, und
- richtet über das Finanz-Clearinghaus **200** ein Anbieterkonto mit wenigstens einer Zahlungsart ein, wie etwa, Kreditkarte, Lastschriftkarte und/oder Bank ein, und
- registriert mehrere Transaktionen mit einer Transaktionsbehörde **700**.

[0486] In diesem Beispiel registriert das Unternehmen mit der Transaktionsbehörde **700**, die eine verteilte Transaktionsbehörde innerhalb des Unternehmens, das die Güter verkauft, sein kann, eine atomare Transaktion, die wenigstens einen elektronischen Regelsatz umfasst, der zum Beispiel folgendes festlegt:

- Das Versenden des Auftrags für das Ausführen durch Durchlaufen von einer oder mehr Organisationen wie etwa ein Lager **1018** und Logistikeinrichtungen **1020** (die zu demselben Unternehmen gehören können oder nicht),
- das Empfangen einer Bestätigung, dass die gewünschte Ware tatsächlich auf Lager ist,
- das Empfangen einer Bestellbestätigung,
- die Vor-Autorisierung für das Bezahlen von einem Zahlungsverfahren für den jeweiligen Kunden, der die Bestellung erteilt hat,
- Anweisungen für den Transport der Ware,
- die Bestätigung, dass die Ware versendet wurde, und
- Regeln für das Abschließen des Zahlungsvorgangs.

[0487] In diesem Beispiel erhält das Unternehmen auch wenigstens ein digitales Zertifikat **504** von einer zertifizierenden Behörde, die wenigstens eine Tatsache attestiert, zum Beispiel,

- dass das Unternehmen eine rechtmäßig im Staat Delaware eingetragene Aktiengesellschaft ist;
- dass das Unternehmen nicht bankrott ist und/oder dass das Unternehmen einen gewissen Grad an Kreditwürdigkeit aufweist,
- dass dem Unternehmen eine Steuernummer zugeteilt wurde, und
- dass das Unternehmen Steuernummern des jeweiligen Bundesstaates in verschiedenen Bundesstaaten, den spezifischen Staaten hat sowie deren entsprechende Identifikationsnummern,

[0488] Ein Kunde **95** verwendet sein oder ihr elek-

tronisches Gerät **100** mit Eigenschaften für das Durchsuchen des Internets, um auf den Katalogserver **1012** über das World Wide Web des Internet zuzugreifen. Der Katalogserver **1012** sendet dem Kunden **95** eine Webseite **1022**, die eine Seite eines elektronischen Katalogs bereitstellt. Webseite **1022** kann in einem oder mehr sicheren elektronischen Containern **152(1)** gesendet werden. Der Kunde **95** zeigt die Webseite **1022A** unter Verwendung seines elektronischen Geräts **100** an und klickt auf den Teil der Webseite, der ein kurzärmliges Oxford Button-down-Männershirt für $15 zeigt. Die aktuelle Webseite wird durch eine Webseite **1022B** ersetzt, die von dem Ausführungsserver kommt. Diese zweite Webseite **1022B** kann in einem sicheren Container **152(2)** versendet werden.

[0489] Das elektronische Gerät des Verbrauchers **100** hat eine geschützte Verarbeitungsumgebung **154**. PPE **154** öffnet den sicheren Container **152** und zeigt die Seite **1022B** auf dem Bildschirm an. Die Seite **1022B**, die nun angezeigt wird, ist ein Formular mit mehreren Feldern einschließlich der Katalognummer und der Beschreibung des Shirts und des Verkaufspreises. Der Kunde **95** füllt Felder bezüglich Farbe, Halsweite, bezüglich der Frage, ob es sich um einen normal große oder sehr große Person, ob das Shirt normal oder eng anliegend sein soll, sowie bezüglich der Menge aus. Der Kunde **95** gibt auch an, ob das Shirt/die Shirts geliefert werden soll(en), die Art des gewünschten Lieferdienstes und die Adresse des Kunden.

[0490] Sobald der Kunde **95** die erforderliche Information vervollständigt hat, gibt das elektronische Gerät **100** die Information **1024** aus den Feldern des Formulars in einen sicheren Container **152(3)** und sendet den Container zurück an den Ausführungsdienst **1014**. Ausführungsserver **1014** öffnet den Container **152(3)** und liest die Feldinformation **1024**. Ausführungsserver **1014** erstellt eine VDE-Audit-Aufzeichnung, der den Empfang der Daten **1024** anzeigt. Ausführungsserver **1014** kann auch einen Regelsatz **188** und/oder eine Ereignisanzeige erstellen, die eine Einkaufstransaktion initiiert.

[0491] Ausführungsserver **1014** kann direkt mit Lager **1018** oder über die Transaktionsbehörde **700** kommunizieren. Der Ausführungsserver **1014** kann dann bestimmen, ob die erforderlichen Güter auf Lager sind und versendet werden können. Wenn Ausführungsserver **1014** bestimmt, dass die benötigten Güter auf Lager sind und versendet werden können, und wenn die von dem Kunden bereitgestellte Information **1024** ausreichend ist, um den Vorgang fortzusetzen, dann sendet der Ausführungsdienst eine andere Webseite **1022C** an den Kunden zurück, die folgendes anzeigt:

- dass der Einkauf ausgeführt werden kann,
- welche Umsatzsteuern und Liefergebühren es jeweils gibt,
- die angegebene Adresse sowie die Art von gewähltem Lieferdienst,
- neue Felder für sich auf die Zahlung beziehende Daten, und
- eine Rückfrage, ob der Kunde fortfahren möchte.

[0492] Der Ausführungsdienst **1014** sendet auch Audit-Aufzeichnung **302(1)** an die PPE **154** des Verbrauchers und an die Transaktionsbehörde **700**, die angibt, welche Teile der größeren atomaren Transaktion ausgeführt wurden.

[0493] Wenn der Kunde **95** beschließt, dass er oder sie nach dem Anzeigen von Ausführungsdetails nicht mit der Transaktion fortfahren möchte, dann kann sein oder ihr Gerät **100** einen sicheren VDE-Container **152(5)** an den Ausführungsserver **1014** und an die Transaktionsbehörde **700** senden und dabei anzeigen, dass die Transaktion abgebrochen wurde. Wenn der Verbraucher **95** sagt, ja, bitte mit der Transaktion fortfahren, dann muss der Verbraucher eine Zahlungsart aus der bereitgestellten Liste auswählen.

[0494] In diesem Beispiel entspricht die Liste Zahlungsarten, die sowohl von dem Anbieter der Waren als auch dem Finanz-Clearinghaus **200** unterstützt werden. Der Kunde **95** trägt zum Beispiel die Kredit- oder Lastschriftkartennummer ein, sowie das Ablaufdatum und die Rechnungsadresse.

[0495] Nach Eintragen der erforderlichen Daten kann das Gerät des Kunden **100** die Daten in einem sicheren VDE-Container **152(2)** unter Verwendung seiner oder ihrer sicheren PPE an das Finanz-Clearinghaus **200** versenden und kann einen gesonderten VDE-Container (nicht gezeigt) mit einer Audit-Aufzeichnung an die Transaktionsbehörde **700** senden.

[0496] Das Finanz-Clearinghaus **200** erhält eine Vorautorisierung von dem Kreditkarten verarbeitenden Unternehmen und sendet zum Beispiel unter Verwendung eines VDE-Containers **152(6)** die Vor-Information über die Zustimmung zur Vorautorisierung **1026** an den Ausführungsserver **1014**. Finanz-Clearinghaus **200** kann einen weiteren VDE-Container **152(7)** mit einer Audit-Aufzeichnung **302(2)** an die Transaktionsbehörde **700** senden, der den Abschluss des Vor-Autorisierungsschritts anzeigt.

[0497] Der Ausführungsserver **1014** kann einen weiteren sicheren VDE-Container **152(8)** mit einer neuen Webseite **1022D** und Audit-Aufzeichnungsdaten **302(3)** an den Kunden **95** senden, wobei die Aufzeichnungsdaten Folgendes angeben:

- dass der Bestellvorgang abgeschlossen ist,
- dass der Verkauf durch die Zahlungsart freigegeben wurde,

• wenn die Güter versendet werden, wird von der Kreditkarte des Kunden der gesamte Betrag abgebucht, und
• eine Transaktionsbestätigungsnummer für das weitere Verfahren, die es ermöglicht, Anfragen an den Ausführungsdienst **1014** und/oder die Transaktionsbehörde **700** zu richten.

[0498] Der Ausführungsdienst **1014** (z. B. in Zusammenarbeit mit Lager **1018**) verpackt die Güter, reicht sie weiter an einen Expresslieferdienst **1020** und sendet zum Beispiel sichere VDE-Container **152(9)**, **152(10)** mit Audit-Aufzeichnungen **302(4)**, **305(5)**, die die Versendung jeweils dem Finanz-Clearinghaus **200** und der Transaktionsbehörde **700** mitteilen. In diesem Beispiel sendet der Expresslieferdienst („Logistik") **1020** auch einen sicheren VDE-Container **152(11)** an die Transaktionsbehörde **700** und an den Ausführungsdienst **1020** (und, wenn gewünscht, auch an den Kunden **95**), der anzeigt, dass der Expressdienst **1020** das Paket übernommen hat.

[0499] Nach Aushändigung des Paktes mit den Waren sendet in diesem Beispiel der Expresslieferservice **1020** einen sicheren VDE-Container **152(12)** mit einer Audit-Aufzeichnung **302(7)**, die anzeigt, dass die Aushändigung des Paktes abgeschlossen wurde, an die Transaktionsbehörde **700**, die dann verzeichnet, dass die Transaktion abgeschlossen wurde, und kann dann zusätzliche sichere VDE-Container **152** versenden, die den Abschluss dem Finanz-Clearinghaus **200**, dem Expresslieferdienst **1020**, dem Ausführungsdienst **1014** und in einigen Beispielen dem Kunden **95** mitteilen.

Beispiel: Das Distributed Commerce Utility **75** kann Transaktionen unterstützen, in denen Kunden für Dienstleistungen bezahlen

[0500] Ein Kennzeichen des westlichen Wirtschaftssystems, insbesondere der Wirtschaft der Vereinigten Staaten am Ende dieses Jahrhunderts, war der Übergang von einer Wirtschaftssystem, das geprägt war durch eine größtenteils fertigende Industrie mit „rauchenden Schornsteinen" nicht nur in eine „Informationswirtschaft" sondern auch in eine „Dienstleistungswirtschaft". Das Distributed Commerce Utility **75** kann Transaktionen unterstützen, in denen Kunden für Dienstleistungen bezahlen, und in vielen Beispielen diese in irgendeiner Weise nützen.

[0501] Fig. 63 zeigt ein Beispiel für ein exemplarisches Dienstleistungssystem **1030**. In einem Beispiel ist ein Online-Dienst **1032** in dem sicheren Verzeichnisdienst **600** registriert und erhält ein digitales Zertifikat **504(1)** von einer zertifizierenden Behörde **500**, das den Online-Dienst identifiziert. Der Online-Dienst vertraut Zertifikaten **504**, die von der zertifizierenden Behörde **500** sowie von Parteien, die von der zertifizierenden Behörde **500** zertifiziert wurden, Zertifikate über bestimmte Tatsachen auszustellen, ausgestellt wurden.

[0502] Zum Beispiel akzeptiert der Online-Dienst **1032** Zertifikate **504(3)**, die von der verteilten zertifizierenden Behörde **500A** ausgestellt werden, von Eltern, die von der zertifizierenden Behörde **500** zertifiziert wurden (über Zertifikat **504(2)**), Zertifikate auszustellen, die belegen, dass sie Kinder haben und dass diese Kinder derzeit noch minderjährig sind. Infolgedessen erlaubt der Online-Dienst **1032** Kindern, die derart zertifiziert wurden, weder den Zugriff auf Themen bestimmten Inhalts, der von dem Online-Dienst vertrieben wird, noch akzeptiert er digitale, auf diesen Zertifikaten basierende Signaturen für Einkaufstransaktionen, außer im Falle, dass der Erziehungsberechtigte des Kindes ein weiteres Zertifikat ausgestellt hat, das attestiert, dass er die finanzielle haftet (z. B. ohne Vorbehalt oder für Einkäufe bis zu einer bestimmten festgelegten Grenze pro Transaktion oder einer bestimmten Gesamthöhe innerhalb eines festgelegten Zeitraums, in einem Beispiel pro Monat). Diese Zertifikate **504(2)**, **504(3)** können von der zertifizierenden Behörde **500** an der Elternteil und/oder wenigstens ein Kind in einem sicheren VDE-Container **152** gesendet werden.

[0503] Man stelle sich nun vor, dass das Kind **95(2)** sich in einem Online-Spiel namens „chat" einträgt. Online-Dienst **1032** hat eine Web-Benutzeroberfläche, deren Gestaltung insbesondere auf Kinder im Schulalter ausgerichtet ist. Dieser Dienst **1032** bietet eine Mitgliedschaft an, die vierteljährlich erneuert werden muss. Unter Verwendung eines elektronischen Geräts **100** wie etwa eines Personal Computers oder TV-Geräts oder einer Settop-Box mit bidirektionaler Kommunikation und einer geschützten Verarbeitungsumgebung **154** verwendet das Kind **95(2)** sichere Verzeichnisdienste **600**, um den Online-Dienst **1032** aufzurufen und schickt eine Nachricht mit dem Mitgliedsantrag an diesen. Als Antwort schickt der Online-Dienst **1032** an den Elternteil **95(1)** oder Erziehungsberechtigten eine Zahlungsaufforderung in einem sicheren VDE-Container **152(4)**, die Mitgliedschaft und die Mitgliedsinformation. Der Elternteil oder Erziehungsberechtigte und/oder die zahlende Privatperson **95(1)** stellt dem Online-Dienst **1032** die Daten **1036** seiner oder ihrer Kreditkartennummer(n), deren jeweiliges Gültigkeitsdatum und Rechnungsadressdaten in einem oder mehr sicheren Containern **152(5)** zur Verfügung.

[0504] In diesem Beispiel teilt der Online-Dienst **1032** die Daten über Kundenkontonummer, Kreditkarte und/oder weitere Zahlungsinformation **1036** dem Finanz-Clearinghaus unter Verwendung eines sicheren VDE-Containers **152(6)** zur Verfügung (in einer Variante dieses Beispiels kann der Elternteil diese Finanzinformation und zugehörige Information direkt dem Finanz-Clearinghaus **200** in einem siche-

ren VDE-Container **152(5)** zur Verfügung stellen). Der Online-Dienst-Anbieter **1032** stellt auch die Clearinghaus-Netzwerkadresse und die Kontonummer des Anbieters bereit. Innerhalb einer geschützten Verarbeitungsumgebung (die zum Beispiel einen Universalcomputer, der in einem physikalisch sicheren Tresor oder einer anderen sicheren Einrichtung verschlossen ist, umfassen kann) öffnet das Finanz-Clearinghaus **200** den sicheren Container **152(6)**, extrahiert die Zahlungsinformation **1036** und schließt die Zahlungstransaktion mit dem Kreditkartenunternehmen ab.

[0505] In diesem Beispiel teilt das Finanz-Clearinghaus **200** wiederum die folgenden Daten **1038** dem Online-Dienst in wenigstens einem sicheren VDE-Container **152(7)** mit (diese Liste dient nur der Veranschaulichung und weicht nicht von dem allgemeinen Fall ab, in dem jegliche verfügbare Menge an Information mitgeteilt werden kann):

- VDE-Audit-Aufzeichnung für diese Transaktion,
- Autorisierungsnummer der Transaktion,
- Kontonummer des Anbieters
- Kundenkontonummer des Kunden bei dem Dienst, und
- zu bezahlender Betrag.

[0506] Daraufhin sendet der Online-Dienst **1032** einen sicheren Container **152(8)** an den Kunden **95(1)**, der anzeigt, dass die Zahlung empfangen wurde. In einem Beispiel kann Online-Dienst **1032** zertifizierender Behörde **500** die Anweisung geben, ein Zertifikat **504** auszustellen, das die Gültigkeit der Mitgliedschaft bis zu einem bestimmten Datum attestiert. Online-Dienst **1032** kann auch von der Information **1038** abgeleitete Audit-Aufzeichnungen **302(1)** bereitstellen, die von dem Finanz-Clearinghaus **200** bereitgestellt wurden.

[0507] Jedes Mal, wenn das Kind **95(2)** sich in den Online-Informationsservice **1032** einloggt, dann überprüft die PPE des Kindes **154**, ob Zertifikate **504** vorliegen oder bekannt sind, und wenn dem so ist, ob:

- diese digitalen Zertifikate eine aktuelle, nicht abgelaufene Mitgliedschaft in dem Online-Dienst belegen, und
- Zertifikate über minderjährige Kinder vorliegen und gültig sind (zum Beispiel nicht abgelaufen sind, weil das Kind noch nicht 18 Jahre alt ist).

[0508] Wenn durch diese Zertifikate **504** sicher gestellt wurde, dass das Kind **95(2)** autorisiert ist, den Online-Dienst **1032** zu nutzen und bestimmte, auf Erwachsene bestimmte Inhalte nicht aufrufen darf, dann gewährt der Online-Dienst einen eingeschränkten Zugang, das heißt, Zugang zu erlaubten Bereichen.

[0509] Unter den Merkmalen dieses Online-Dienstes sind verteilte, interaktive Spiele für mehrere Personen. Das Kind **95(2)** spielt das Spiel in diesem Beispiel mit wenigstens einem anderen autorisierten und zertifizierten minderjährigen Kind – Erwachsene sind in diesem speziellen Beispiel durch VDE-Regeln und Steuermechanismen von dem Spiel ausgeschlossen. Zumindest ein Teil der Software (z. B. ausführbarer Code und/oder interpretierbarer Code, wie etwa Java), der wenigstens einen Bereich **1040** des wenigstens einen Spiels implementiert, kann von dem Online-Dienst **1032** auf das Datengerät **100(2)** des Kindes unter Verwendung von wenigstens einem sicheren VDE-Container **152(9)** heruntergeladen werden.

[0510] Unter Verwendung von in der Ginter et al. beschriebenen Offenbarung wird festgelegt, dass diese Programme und/oder Teile von Programmen **1040** authentisch und unverändert sein müssen. Wenigstens einer der Schlüssel, die verwendet werden, um die Einweg-Hashfunktion welche die digitale Signatur erzeugt, die für das Bestimmen der Integrität des wenigstens einen Programms **1040** oder wenigstens einen Programmteils verwendet wird, ist über ein von der zertifizierenden Behörde **500** ausgestelltes Zertifikat **504** mit der Kennung des Online-Dienstes **1032** verknüpft.

[0511] Wenn das Kind **95(2)** in diesem Beispiel das Spiel spielt, dann wird zumindest ein Teil seiner oder ihrer Aktivitäten gemäß den Verfahren der anhängenden Anmeldung von Ginter et al. gemessen, und Audit-Aufzeichnungen **302(2)**, die die Benutzungseigenschaften des Kindes anzeigen, werden erstellt. Zu bestimmten Zeitpunkten werden diese Audit-Aufzeichnungen **302(2)** an den Online-Dienst **1032** übertragen, der in diesem Beispiel ein Usage-Clearinghaus **300** einschließen kann. Usage-Clearinghaus **300** analysiert diese Benutzungsaufzeichnungen **302(2)** und kann sie verwenden, um zu bestimmen, wie viel Kind **95(2)** bezahlen muss.

Beispiel: Das Distributed Commerce Utility **75** kann verwendet werden, um eine Disaggregation der Wertkette für Einkauf und/oder Verwendung von materiellen Gütern bereitzustellen

[0512] Das Distributed Commerce Utility **75** kann verwendet werden, um den Einkauf oder eine andere Art einer auf materielle Güter bezogenen Transaktion zu vereinfachen. Fig. 64 zeigt ein Beispiel für ein System für den Verkauf von materiellen Gütern **1040**. Zum Beispiel erteilt ein Unternehmen **1042** eine Bestellung für Bürobedarf und verwendet dazu ein elektronisches Gerät **100** einschließlich einer PPE **154**. Die Bestellung beläuft sich auf eine Schachtel Büroklammern, einen Hefter, Heftklammern, eine Schachtel Kopierpapier mit den Maßen 8,5 × 11 Inch und ein Dutzend gelbe Folio-Note Pads. Die Produkte werden von einem Hersteller **1050** hergestellt, von einem Vertriebshändler **1048** vertrieben und von einem Ein-

zelhändler **1046** an das Unternehmen verkauft.

[0513] In diesem Beispiel erhält ein Finanz-Clearinghaus **200** eine Bezahlung **1052** von dem Unternehmen **1042** und disaggregiert die Bezahlung, indem es sie in disaggregierte Zahlungen **1052A**, **1052B**, **1052C** aufteilt, die es jeweils an Einzelhändler **1046**, den Verteiler **1048** und den Hersteller **1050** aushändigt.

[0514] Zum Beispiel sendet das Unternehmen **1042** seinen Auftrag **1044** innerhalb des sicheren VDE-Containers **152(1)** an einen Einzelhändler **1046**. In diesem Beispiel stellt Einzelhändler **1046** einen Ausführungsdienst bereit, der den Auftrag **1044** erhält und daraufhin einen Regelsatz **188** bereitstellt, der die Anbieterkontonummer des Verteilers **1048** und/oder Herstellers **1050** jedes Produktes und den Prozentsatz des Verkaufspreises, den jeder erhält, angibt. Gegebenenfalls kann der Einzelhändler **1046** einen anderen Regelsatz **188** für jedes bestellte Produkt bereitstellen (unabhängig von der Menge), der es dann ermöglicht, eine unterschiedliche Zahlungsdisaggregation je nach Produkt durchzuführen. Einzelhändler **1046** kann diesen Regelsatz **188a** einem Unternehmen **1042** zur Verfügung stellen.

[0515] Regelsatz **188a** kann auf das Vorhandensein von einem oder mehr digitalen Zertifikaten **504**, die von zertifizierender Behörde **500** ausgestellt wurden, eingestellt werden. Zum Beispiel kann Regelsatz **188a** Unternehmen **1042** auffordern, ein digitales, von der zertifizierenden Behörde **500** ausgestelltes Zertifikat **504(1)** vorzulegen. Zertifikat **504(1)** attestiert die Identität des bestellenden Unternehmens **1042**. Das Unternehmen **504(1)** kann ein anderes Zertifikat **504(2)** in derselben Kette der Vertrauenswürdigkeitshierarchie als zertifizierende Behörde bereitstellen, das gewährleistet, dass die bestellende Person autorisiert ist, Bestellungen bis zu einer gewissen Bestellgrenze pro Bestellung zu erteilen. Unternehmen **1042** kann auch dasselbe oder ein anderes Zertifikat **504(2)** bereitstellen, das auch angibt, dass der Angestellte des Einkäufers innerhalb des Unternehmens autorisiert ist, die Lastschriftkarte des Unternehmens zu verwenden.

[0516] In diesem Beispiel bezahlt das Unternehmen **1042** mit einer Lastschriftkarte des Unternehmens. Das Finanz-Clearinghaus **200** erhält zunächst eine Zahlungsautorisierung von dem Kreditkartenunternehmen, bevor der Einzelhändler **1046** die Ware versendet. Nach dem Erhalt der Benachrichtigung über die Vorautorisierung kann Einzelhändler **1046** die Güter **1047** an das Unternehmen **1042** versenden. Nach dem Ausliefern der Ware **1047** erstellt der Einzelhändler **1046** wenigstens eine VDE-Audit- und/oder Rechnungsaufzeichnung **1052** in wenigstens einem sicheren VDE-Container **504(2)** und überträgt den Container an das Finanz-Clearinghaus **200** (Auditdaten können alternativ auch an den Einzelhändler **1046** versendet werden).

[0517] Das Finanz-Clearinghaus **200** schließt dann die Lastschriftkartentransaktion ab, indem es den Gesamtbetrag jedem durch Regelsatz **188a** festgelegten Teilnehmer der Wertkette zuteilt (den Gesamtbetrag hat es entweder direkt von Einzelhändler **1046** und/oder Unternehmen **1042** erhalten). Auf diese Weise erhalten die Verteiler **1048** und oder Hersteller **1050** zur gleichen Zeit wie der Einzelverkäufer **1046** die Zahlung. Regelsatzinformation **188a** kann auch Teilungen der Gesamtzahlung und Kontonummern des Anbieters für lokale, bundesstaatliche und gesamtstaatliche Steuern, wenn diese gezahlt werden, und zum Beispiel für Lieferkosten angeben, wie etwa an ein Overnight-Express-Unternehmen, wenn derartige Lieferkosten zu zahlen sind.

[0518] Dieses in Fig. 64 dargestellte Beispiel zeigt, dass die Disaggregation der Wertkette sowohl auf materielle als auch auf immaterielle Güter angewendet werden kann. Ähnliche Techniken können auch sehr viel weiter vorne in der Lieferkette des Herstellers **1050** angewendet werden, wenn dies gewünscht wird (z. B. auf die Anbieter des Metalls, aus dem die Büroklammern hergestellt wurden).

Beispiel – Das Distributed Commerce Utility **75** kann die Verteilung digitalen Eigentums durch Bereitstellen einer Objektregistrierungsfunktion sowie weiteren Diensten unterstützen.

[0519] Das Distributed Commerce Utility **75** kann die elektronische Gemeinschaft darin unterstützen, elektronisches oder digitales Eigentum oder Inhalte effizient zu verteilen. Zum Beispiel sendet ein Ersteller oder anderer Rechteinhaber **400** für die Registrierung unter Verwendung eines elektronischen Geräts **100** mit einer sicheren Verarbeitungseinheit **154** ein digitales Objekt in einem sicheren Container an ein Rechte- und Berechtigungs-Clearinghaus **400**.

[0520] Das Rechte- und Berechtigungs-Clearinghaus **400** öffnet den Container, zum Beispiel unter Verwendung seiner eigenen geschützten VDE-Verarbeitungseinheit und teilt eine einheitliche Objektkennung, welche die Identität des Erstellers, die registrierte Objektart – Software, Video, Sound, Text, Multimedia, etc. – angibt, sowie die digitale Signatur für das Objekt zu. Die einheitliche Objektkennung kann global einheitlich sein oder nur in der Namensraumdomäne des Erstellers oder einer anderen Einheit, wie etwa eines Online-Dienstes, einer digitalen Bibliothek oder einer speziellen Gerichtsbarkeit, wie etwa eines jeweiligen Landes, einheitlich sein.

[0521] In diesem Beispiel signiert das Rechte- und Berechtigungs-Clearinghaus **400** die einheitliche Objektkennung digital mit dem geheimen Schlüssel des

Rechte- und Berechtigungs-Clearinghauses und sendet das Objekt sowie die Kennung an die Person oder Organisation zurück und registriert es dafür in einem sicheren VDE-Container. Das Rechte- und Berechtigungs-Clearinghaus **400** kann eine Kopie des Objekts zurückbehalten oder lediglich die einheitliche Objektkennung für das Objekt sowie die Signaturen für das Objekt und dessen einheitliche Objektkennung zurückbehalten. In einem weiteren Beispiel signiert das Rechte- und Berechtigungs-Clearinghaus **400** digital ein neues Objekt, das aus dem ursprünglichen Objekt und dessen einheitlicher Dateikennung besteht und speichert sowohl das neue Objekt und/oder dessen Signatur in dem Archiv des Rechte und Berechtigungs-Clearinghauses **400**.

[0522] Der Ersteller kann auch ein Berechtigungs- und Preisbildungstemplate **450** in einem sicheren VDE-Container gesendet haben (siehe Fig. 45A-Fig. 45C), das angibt, welche Berechtigungen gewährt werden, die Preise, die für das Ausüben dieser Berechtigungen entfallen und wenn möglich, die Einzelperson, Klasse und/oder Gerichtsbarkeit, für die diese Preise und Berechtigungen gültig sind. Mehr als ein Berechtigungs- und Preisbildungstemplate **450** kann in einem einzelnen sicheren VDE-Container **152** gesendet werden, oder einzelne sichere VDE-Container **152** können für jedes Berechtigungs- und Preisbildungstemplate verwendet werden.

[0523] In diesem Beispiel wird das Objekt dann unter Verwendung eines sicheren VDE-Containers **152** von dem Ersteller an einen Verteiler **168** übertragen (siehe **Fig.** 16). Unter Verwendung eines Zertifikats **504** kann der Verteiler **168** dann der VDE-Ebene (PPE **154**), die den Regelsatz des Erstellers interpretiert, beweisen, dass der Verteiler tatsächlich autorisiert ist, selektiv Berechtigungen und Preise des Objekts zu verändern und erstellt ein neues Berechtigungs- und Preisbildungstemplate. Der Verteiler **168** sendet dann einen sicheren VDE-Container an das Rechte- und Berechtigungs-Clearinghaus **400**, das die einheitliche Objektkennung sowie die neuen Regeln enthält. In der bevorzugten Ausführungsform hat der Verteiler **168** die Möglichkeit, wenn das Objekt unverändert bleibt, die einheitliche Objektkennung unverändert zu lassen, wenn jedoch der Verteiler das Objekt verändert hat, eventuell um seine eigene Kennzeichnung hinzuzufügen, dann muss die einheitliche Objektkennung verändert werden, um die Fassung des Verteilers zu zeigen. Die digitale Signatur wird erneut mit dem nicht-öffentlichen Schlüssel des Verteilers berechnet. Wie zuvor hat die Objektregistrierung die Möglichkeit, nur die digitale Signatur oder sowohl die Signatur als auch das aktuelle Objekt zu speichern.

Beispiel – Das Distributed Commerce Utility **75** kann verwendet werden, um die Registrierung von Urheberrechten zu vereinfachen

[0524] Als ein Mehrwertdienst kann das Rechte- und Berechtigungs-Clearinghaus **400** einen Dienst für das Registrieren von Urheberrechten bereitstellen (siehe Fig. 43). Das Rechte- und Berechtigungs-Clearinghaus **400** kann eine Kopie des Objekts an den entsprechenden Online-Dienst für das Registrieren von Urheberrechten der entsprechenden Regierungsbehörde **440**, zum Beispiel das US-Copyright Office, schicken. Das Objekt und die einheitliche Objektkennung können in einem sicheren VDE-Container zusammen mit den Regeln, welche die Zahlungsart angeben versendet werden, falls eine Registrierung oder Verarbeitung in Rechnung gestellt wird.

[0525] In diesem Beispiel kann der Dienst für das Registrieren von Urheberrechten wenigstens einen sicheren VDE-Container an das Finanz-Clearinghaus **200** mit wenigstem einer Audit-Aufzeichnung, die den zu zahlenden Betrag, die Zahlungsart sowie das Konto der registrierenden Partei, und das Konto der Regierung, die das Geld erhalten soll, angibt, und erhält im Gegenzug eine Audit-Aufzeichnung in einen sicheren VDE-Container, die angibt, dass die Transaktion vor-autorisiert wurde (oder dass aus irgendeinem Grund die vorgeschlagene Transaktion nicht genehmigt wurde).

[0526] Wenn die Transaktion von dem Finanz-Clearinghaus **200** vor-autorisiert wurde, dann öffnet ein VDE-fähiger Computer, der sich in diesem Beispiel in dem US-Copyright Office befindet, den sicheren Container und fügt die einheitliche Objektkennung und das Objekt der Registrierungsdatenbank hinzu. In einer Kette des Vertrauens (Chain of Trust), die von der zertifizierenden Behörde **500** ausgeht, die in diesem Beispiel von oder in Auftrag der US-Regierung betrieben werden kann – gibt der Dienst für das Registrieren von Urheberrechten wenigstens ein digitales Zertifikat **504** aus, das gleichzeitig mit der Registrierung eines Objekts attestiert, dass das Objekt mit einer spezifischen digitalen Signatur tatsächlich bei der Registrierungsbehörde registriert wurde und dass die wenigstens eine Person zu der Zeit, als das Objekt registriert wurde in der Tat der Eigentümer des Urheberrechts war. Dieses Zertifikat **504** wird an einen sicheren VDE-Container an die Person gesendet, die das Objekt registriert hat (und/oder die als die zu benachrichtigende Person angegeben wurde), sowie an das Rechte- und Berechtigungs-Clearinghaus **400**, das wiederum Daten bezüglich der Registrierung von Urheberrechten in einem sicheren VDE-Container bereitstellen kann.

[0527] Der Dienst für das Registrieren von Urheberrechten sendet wenigstens einen sicheren VDE-Con-

tainer an das Finanz-Clearinghaus **200** mit wenigstens einer Audit-Aufzeichnung, die das Finanz-Clearinghaus **200** anweist, mit der Ausführung der vor-autorisierten Transaktion fortzufahren (wenn sämtliche notwendige Daten Teil des Vor-Autorisierungsprozesses waren) und/oder stellt Daten bezüglich zum Beispiel des zu zahlenden Betrags, der Zahlungsart und dem Konto der registrierenden Partei, dem Konto der US-Regierung für das Erhalten der Gelder für das Clearinghaus **200** und teilt mit, dass die Zahlungstransaktion abgeschlossen werden soll, und erhält im Gegenzug von dem Finanz-Clearinghaus eine Audit-Aufzeichnung in einem sicheren VDE-Container, die angibt, dass die Transaktion beendet wurde und dass Gelder an die jeweiligen Konten/das jeweilige Konto überwiesen wurden, oder dass die Zahlungstransaktion fehlgeschlagen ist und der Grund, warum sie nicht abgeschlossen werden konnte.

Beispiel – Das Distributed Commerce Utility **75** kann Aktualisierung oder Veränderung von Berechtigungen und Preisen unterstützen

[0528] Das Distributed Commerce Utility **75** kann ferner die Verteilung von elektronischem und digitalem Eigentum durch das Bereitstellen eines Mechanismus für das Erneuern von Rechten und Berechtigungen, die abgelaufen sind, vereinfachen. Siehe Fig. 42A.

[0529] In einem Beispiel sei angenommen, dass ein Angestellter eines Fortune-Unternehmens **1000** einen Regelsatz für ein digitales Eigentum hat, vielleicht einen Teil einer Software oder ein Java-Applet, der abgelaufen ist. Die geschützte VDE-Verarbeitungsumgebung auf dem Computer des Angestellten kann einen sicheren VDE-Container an das Rechte- und Berechtigungs-Clearinghaus **400** senden.

[0530] Das Distributed Commerce Utility **75** kann ferner die Verteilung von elektronischem und digitalem Eigentum durch das Bereitstellen eines Mechanismus für das Verteilen von Rechten, Berechtigungen und Preisen, die von einem oder mehr Teilnehmern in einer Verteilungskette geändert wurden, vereinfachen. In einem Beispiel stelle man sich vor, dass sich auf der Festplatte einer Kundin ein digitales Objekt sowie dessen VDE-Regelsatz, wie er von dem Herausgeber ausgegeben wurde, befinden. Die Berechtigungen und Preise sahen ursprünglich ein Pay-per-Use-Modell vor, bei dem der Benutzer 10 Cent für jeden mit dem Objekt durchgeführten Vorgang wie Drucken oder Anzeigen bezahlt.

[0531] Um zu bestimmen, ob die neuen Rechte und Preise nun verfügbar sind, kann die geschützte Verarbeitungsumgebung am PC des Kunden unter Verwendung seiner Netzwerkadresse, die es von dem Regelsatz zusammen mit MIME-fähiger elektronischer Mail erhalten hat, einen sicheren VDE-Container an das Rechte- und Berechtigungs-Clearinghaus **400** senden. Der Kunde erhielt die Adresse des Rechte- und Berechtigungs-Clearinghauses von dem sicheren Verzeichnisdienst **600** dadurch, dass er zum Beispiel eine Anfrage in einem sicheren VDE-Container versendet hat und dadurch, dass er eine Antwort in dem sicheren VDE-Container erhalten hat.

[0532] Der Verteiler **400** sendet dann einen sicheren VDE-Container an das Rechte- und Berechtigungs-Clearinghaus, das die einheitliche Objektkennung sowie eine Anforderung der aktuellen Regeln einschließlich der Preise enthält. Die geschützte Verarbeitungsumgebung auf dem Server des Rechte- und Berechtigungshauses **400** öffnet den sicheren VDE-Container, ruft den aktuellsten Regelsatz von der Regelsatz-Datenbank auf und sendet über eine automatisch generierte elektronische Mail (Return Electronic Mail) einen weiteren sicheren VDE-Container mit den gewünschten Regeln. Die geschützte Verarbeitungsumgebung des Kunden öffnet diesen Container und ersetzt und/oder erweitert die abgelaufenen Regeln durch die neuen. Der Kunde kann nun den Inhalt gemäß den Regeln und Steuermechanismen, die in dem gerade erhaltenen Regelsatz von dem Rechte- und Berechtigungs-Clearinghaus festgelegt und von der VDE-Ebene des lokalen Computers oder einer anderen Anwendung verarbeitet wurden, verwenden. In diesem Beispiel haben neue Regeln und Steuermechanismen den Pay-per-Use-Preis von zehn Cent pro Vorgang auf fünf Cent pro Vorgang herabgesetzt.

Beispiel – Das Distributed Commerce Utility **75** kann Modelle für das Verteilen neuer Rechte unterstützen

[0533] Das Distributed Commerce Utility **75** kann auch Transaktionen unterstützen, in denen einige oder alle Rechte nicht von Anfang an den Endkunden mit dem Inhalt verteilt werden sondern erst angefordert werden müssen. In einem Beispiel stelle man sich vor, dass ein Rechtsanwalt sich entscheidet, in das Druckgeschäft einzusteigen indem er seine/ihre Artikel mit anderen Materialien aus legalen Informationsverteilern kombiniert. Die legalen Verteiler von Information haben ein Rechte- und Berechtigungs-Clearinghaus **400** ausgewählt, ihr Verteiler für Regelsatzdaten für ihre vielen Eigentümer zu sein. Mit jedem Objekt, das sie bei dem Rechte- und Berechtigungs-Clearinghaus **400** registrieren, registrieren sie auch zwei Regelsätze in den Formaten, die in der Patentschrift von Ginter et al. beschrieben wurden.

- ein Regelsatz legt Standardregeln einschließlich Preisen für Einzelverkäufer, fest, und
- ein zweiter Regelsatz überträgt Rechte und Preise, die seltener von Interesse sind an den Einzelverkäufer, zum Beispiel, die Berechtigung für das Erstellen einer Anthologie.

[0534] Der Herausgeber des Newsletters für Anwälte erhält ein Kapitel einer Abhandlung über Patentrecht und will einen Auszug von 1000 Wörtern in dem Newsletter zusammen mit anderen Artikeln einschließen. Da der Herausgeber des Newsletters bereits das Abhandlungskapitel erhalten sowie den Regelsatz für den Verkauf erhalten hat, sendet er eine Anfrage in einem sicheren VDE-Container unter Verwendung einer Internet MIME-fähigen E-Mail an das Rechte- und Berechtigungs-Clearinghaus **400** und bittet um das Recht für das Exzerpieren sowie für das Anthologisieren des durch die beigefügte einheitliche Objektkennung identifizierten Kapitels zu erstellen. Der Anwalt hat das Rechte- und Berechtigungs-Clearinghaus **400** unter Verwendung eines sicheren Verzeichnisdienstes **600** gefunden (alternativ kann die Adresse des Rechte- und Berechtigungs-Clearinghauses in der ursprünglichen Verkaufsversion, die der Anwalt erhalten hat, enthalten sein).

[0535] Das Rechte-Clearinghaus **400** überprüft die Objektdatenbank, lokalisiert die Regelsatzinformation für das in der allgemeinen Objektkennung benannte Objekt, und stellt fest, dass sowohl die Rechte für das Exzerpieren als auch für das Anthologisieren zusammen mit den Preisen für jedes dieser Rechte verfügbar sind. Das Recht auf das Exzerpieren erteilt keine Berechtigung, den als Auszugs verwendeten Teil zu verändern. Das Recht auf das Anthologisieren wird zusammen mit Regeln übertragen, die den Preis auf einen 30%-igen Rabatt vom Kaufpreis herabsetzen, der für die Länge eines Auszugs bezahlt werden muss, falls nicht das gesamte Kapitel für die Anthologie verwendet wird.

[0536] Unter Verwendung einer VDE-fähigen Anwendung für das Zusammenstellen von Seiten stellt der Newsletter-Herausgeber verschiedene Werke in einem neuen Werk zusammen, einschließlich des Auszugs von 1000 Worten, und registriert das neue Objekt bei dem Rechte- und Berechtigungs-Clearinghaus zusammen mit seinem Regelsatz oder seinen Regelsätzen. Der Newsletter-Herausgeber registriert auch das neue Objekt mit einer Funktion für das Registrieren von Urheberrechten, zum Beispiel dem US-Patent and Copyright Office (amerikanisches Patentamt). Der Newsletter-Herausgeber verteilt das neue Werk in einem sicheren VDE-Container, der auch Regelsätze für jedes der einzelnen anthologisierten Werke sowie für den gesamten Newsletter enthält. Die lokale geschützte VDE-Verarbeitungsumgebung auf dem Gerät des Benutzers verfolgt die Benutzung gemäß den Regeln, die für das zusammengestellte Objekt gültig sind und gemäß den Regeln für seine Bestandteile, für die getrennte Regeln existieren. Zu bestimmten Zeiten schickt die VDE-Ebene Audit-Aufzeichnungen an das Benutzungs-Clearinghaus **300** sowie an das Finanz-Clearinghaus **200**.

Beispiel – Das Distributed Commerce Utility **75** kann elektronische Rechteverhandlung (Electronic Rights Negotiations) unterstützen

[0537] In einem Beispiel erstellt ein Professor ein "Kurspaket": eine Zusammenstellung vieler verschiedener Werke, die von Studenten in einem bestimmten Kurs verwendet werden sollen, der in diesem Beispiel nur ein Semester dauert. In diesem Beispiel sendet der Professor einen sicheren VDE-Container mit einer Anfrage an das entsprechende Rechte- und Berechtigungs-Clearinghaus **400** und bekommt einen Regelsatz für die in der Anfrage aufgelisteten digitalen Eigentümer zurückgeschickt. Nach dem Erhalt der Berechtigungen und Preise bemerkt der Professor, dass ein Kapitel aus einem Buch einen Preis hat, durch den der Gesamtpreis des Kurspakets über dem Höchstpreis liegt, den er/sie festgelegt hat.

[0538] Unter Verwendung der Verhandlungsmechanismen, die in Ginter et al. offenbart wurden (siehe, zum Beispiel Fig. 7A-76B), versucht der Professor mit dem Rechte- und Berechtigungs-Clearinghaus **400** zu verhandeln. Das Rechte- und Berechtigungs-Clearinghaus **400** wiederum bestimmt automatisch, dass es nicht berechtigt ist, zu verhandeln und leitet die Verhandlung auf den Herausgeber um.

[0539] Nach Erhalt eines geeigneten Zertifikats **504** von einer zertifizierenden Behörde **500** durch das Bereitstellen von Credentials, die die Mitgliedschaft in der Klasse "Hochschulen" anzeigen, unterbreitet die geschützte Verarbeitungsumgebung des Webservers des Herausgebers ein Angebot über einen neuen, veränderten Regelsatz für das für diesen Professor bestimmte Eigentum. Die Regeln haben einen herabgesetzten Preis, erfordern, dass die Kopien auf einem VDE-fähigen, autorisierten Drucker gedruckt werden, der die Anzahl der Kopien überwacht und erstatten den verschiedenen an der Transaktion beteiligten Parteien unter Verwendung von VDE-Techniken Bericht. Der Professor ist nach wie vor unzufrieden mit dem Preis und sendet ein VDE-Verhandlungs-Gegenangebot in einem sicheren Container an den Herausgeber. Die VDE-Ebene des Herausgebers verhandelt mit dem Regelsatz für die Verhandlung über das Gegenangebot des Professor und wenn eine Einigung erzielt wird, stellt sie einen neuen Regelsatz mit den neuen vereinbarten Preisen und Geschäftsbedingungen für den Professor bereit, der dann damit fortfährt, das Kurspaket zu erstellen. Das Rechte- und Berechtigungs-Clearinghaus **400** gewährt den herabgesetzten Preis, weil der Professor in diesem Beispiel in der Lage ist, ein digitales Zertifikat vorzulegen, das beweist, dass er eine Vollzeitstelle an der University of California, Los Angeles hat und dass eine bestimmte Mindestanzahl von Studenten diese Materialien verwenden werden. Diese Authentifizierung entspricht Anforderungen, die dem Rechte- und Berechtigungs-Clearinghaus **400** von dem

Herausgeber mitgeteilt wurden.

Beispiel – Zertifizierung von ausführbaren Dateien (executables)

[0540] Ein wertvoller Nutzen der zertifizierenden Behörden **500** besteht im Ausstellen von digitalen Zertifikaten im Auftrag der Regierung. Zusätzlich zu dem Ausstellen der Zertifikate, die die Identität, den Familienstand etc. belegen, könnten zertifizierende Regierungsorganisationen **500** Zertifikate ausstellen, die ausführbare Regeln zertifizieren, zum Beispiel Lademodule. Zum Beispiel könnten zertifizierende Regierungsbehörden **500** auf allen Ebenen den Satz von ausführbaren Dateien zertifizieren, der die Gesetzes- und Handelsvorschriften ihrer Verwaltungsdistrikte repräsentiert. Zum Beispiel könnte man in Saudi-Arabien darauf bestehen, dass sämtliche Geräte in ihrer Verwaltungsbehörde Lademodule aufweisen, die von der Regierung zertifiziert sind und die Attribute von Containern untersuchen, um sicherzustellen, dass nur geeignete Inhalte freigegeben werden. Der Staat Kalifornien könnte ein Lademodul zertifizieren, das die Steuer dieses Bundesstaates etc. berechnet.

Beispiel: Vertrieb von Unterhaltungsmedien

[0541] Das Distributed Commerce Utility **75** kann verwendet werden, um effizient und flexibel Modelle für den Filmvertrieb auf dem Kundenmarkt zu unterstützen. Zum Beispiel will ein Film- und Unterhaltungsunternehmen wie etwa Disney ein elektronisches Distributed Commerce Utility **75** bereitstellen, um den Vertrieb seiner Filme an seine Kunden **95** zu unterstützen. Disney könnte selbst ein Commerce Utility System **90** eröffnen, oder könnte einen Vertrag mit einer neutralen dritten Partei abschließen, die in seinem Auftrag Commerce Utility Systeme bereitstellen soll. Der Zweck des Commerce Utility Systems **90** ist in diesem Beispiel, sicheres Pay-per-View/Pay-per-Use, Verleihen, Leasing und andere Filmvertriebstransaktionen an Kunden zu unterstützen.

[0542] Die Filme selbst könnten in digitalisierter linearer Form vertrieben werden – zum Beispiel auf DVDs oder auf anderen Medien mit hoher Speicherkapazität. Derartige Medien speichern zusätzlich zu den Filmen selbst, einen oder mehr sichere Container einschließlich Regelsätzen für das Steuern der Benutzung der Filme. Verbraucher **95** könnten die Filme bezahlen, indem sie einen Media Player **104** (siehe Fig. 1) verwenden, der eine Netzwerkverbindung **150** oder einen anderen "Back Channel" (z. B. die Fähigkeit, von einer Smart Card oder ähnlichem zu lesen oder darauf zu schreiben) aufweist.

[0543] Media Player **104** hat eine geschützte Verarbeitungsumgebung **154**, wie etwa eine sichere Verarbeitungsumgebung für die Verwendung beim Verwalten von Rechten und das Handhaben der elektronischen Container. Das Speichermedium kann auch von einem Personal Computer **124**, der mit einer geschützten Verarbeitungsumgebung und einer Netzwerkverbindung ausgestattet ist, abgespielt werden.

[0544] Settop-Box **104** kann über elektronische Steuermechanismen gesteuert werden, die auf den Medien und/oder über den Back Channel verteilt werden. Die Regeln bewirken, dass Settop-Box **104** die Benutzung durch den Verbraucher und die Zahlungsdaten für jedes Eigentum, das der Verbraucher anzeigen möchte, aufzeichnet. Zum Beispiel könnte ein Verbraucher **95** ein Medium wie etwa eine optische DVD in einen Media Player **104** legen und den "Play"-Knopf drücken. Der Media Player **104** des Kunden könnte als nächstes eine Nachricht anzeigen (z. B. über den Fernseher), die den Verbraucher darüber in Kenntnis setzt, wie viel es kostet, diesen speziellen Film anzuschauen (z. B. $2.95) und den Verbraucher fragen, ob er fortfahren möchte. Wenn der Verbraucher mit „Ja" antwortet, dann wird Media Player **104** den Film auf dem Fernsehanlage **102** des Verbrauchers abspielen – und die Benutzungs- und Bezahlungsdaten für die Berichterstattung an Commerce Utility System **90** aufnehmen. Die geschützte Verarbeitungsumgebung **154** innerhalb von Media Player **104** kann unter sicherer Steuerung durch einen oder mehr assoziierten elektronischen Regelsätzen, die an dieselbe gesendet wurden, eine Überwachung und Erfassung von Daten durchführen, die letztendlich verwendet werden können, um sicherzustellen, dass der Verbraucher für das Anschauen des Films bezahlt sowie um eine sichere Benutzungsprüfung durchzuführen. Die sichere Benutzungsprüfung kann zum Beispiel verwendet werden, um es Disney, den Schauspielern und dem Regisseur des Films und anderen Mitwirkenden zu ermöglichen, sicher herauszufinden, wie viele Verbraucher den Film angeschaut haben (und auch um potenziell demographische Daten für das Abstimmen der Werbung auf bestimmte Zielgruppen oder ähnliches zu sammeln). Zum Beispiel kann die geschützte Verarbeitungsumgebung des Media Players **104** sicher die folgenden Daten mittels eines Benutzungszählers, von Rechnungs- und oder Budgetbuchungsprüfungen, die mit den jeweiligen Regeln verknüpft sind, erfassen und aufzeichnen:

- Titel des Films
- digitale Kennung des Films
- Uhrzeit und Datum des Abspielens des digitalen Eigentums
- Anzahl der Abspielvorgänge des digitalen Eigentums
- welche Person den Film abgespielt hat

[0545] In einem Beispiel müssten Verbraucher **95** ein digitales Zertifikat **122** besitzen, das von einer entsprechenden zertifizierenden Behörde ausgestellt

wurde und das für den Nachweis bestimmter Tatsachen dient. Ein derartiges digitales Zertifikat **122** kann verwendet werden, um einen Kontext für elektronischen oder mehrere elektronische Regelsätze, die an Media Player **104** gesendet werden, bereitzustellen. Ein derartiges Zertifikat könnte vorliegen, bevor es dem Verbraucher erlaubt ist, den Film ab zu spielen und/oder um zu verhindern, dass der Film unter bestimmten Bedingungen abgespielt wird und/oder um die Regeln anzuwenden, die gelten, wenn der Film abgespielt wird.

[0546] Zum Beispiel könnten die Eltern ein digitales Zertifikat **122** erhalten, das anzeigt, dass es Kinder in ihrem Haushalt gibt. Das digitale Zertifikat **122**, das anzeigt, dass ein Kind vorhanden ist, könnte verhindern, dass auf Media Player **104** keine anderen Filme als solche mit "G"- oder "PG"-Einstufungen (G rating: entspricht dem Deutschen „Freigegeben ohne Altersbeschränkung; R rating: empfiehlt eine vorherige Begutachtung oder Freigabe durch einen Elternteil) abgespielt werden können. Derartige Zertifikate **122** könnten von derselben Organisation ausgestellt werden, die gegebenenfalls die anderen Verwaltungs- und Unterstützungsdienste in Verbindung mit diesem Beispiel bereitstellen.

[0547] Die elektronischen Regeln, die mit einem bestimmten Film auf einem Medium wie etwa einer optischen Disk bereitgestellt werden, könnten auch eine bestimmte Disaggregation der Wertkette festlegen, die im Zusammenhang mit Zahlungsvereinbarungen angewendet werden soll. Zum Beispiel würde der Media Player **104** von den an ihn gesendeten elektronischen Regeln und Steuermechanismen "wissen", dass der Verteiler, das Studio und das Distributed Commerce Utility **75** bestimmte einen bestimmten Prozentsatz der Benutzungsgebühr von $2.95 erhalten sollen und dass eine staatliche Regierungsbehörde eine bestimmte Steuer in Form von Umsatzsteuer oder Mehrwertsteuer erhält. Da diese Information in der geschützten Verarbeitungsumgebung **154** in dem Media Player **104** gespeichert wird, kann es sein, dass die Verbraucher niemals mit dem Ablauf der Zahlungsdisaggregation und/oder deren Details in Berührung kommen. (Normalerweise wissen Verbraucher nicht, dass das, was der Verteiler einnimmt nichts mit dem zu tun hat, was das Filmstudio bekommt. Die geschützte Verarbeitungsumgebung innerhalb von Media Player **104** kann diese Zahlungsdisaggregation lokal oder über eine verteilte oder zentrale Finanz-Clearing-Funktion **200** wie oben beschrieben bereitstellen.)

[0548] Media Player **104** kann die von ihm erfasste enthaltene Benutzungsinformation auf Echtzeit- (Online) und/oder periodischer ereignisgesteuerter Basis übermitteln. In einem Beispiel kann der Media Player am Ende jedes Monats die von ihm über den vorangehenden Monat erfassten Daten übermitteln. Er kann die erfassten Zahlungsdaten (einschließlich von dem Regelsatz bereitgestellten Disaggregationsdaten) an ein von Disney betriebenes Finanz-Clearinghaus **200** übermitteln (oder derartige Daten können direkt an das Clearinghaus **200** übermittelt werden). Finanz-Clearinghaus **200** stellt sicher, dass das Konto des Kunden entsprechend belastet wird und dass die verschiedenen Zahlungsempfänger (z. B. Disney, der Filmverteiler und andere Teilnehmer in der Wertkette entsprechende Anteile der Zahlung an den Verbraucher erhalten. Das Finanz-Clearinghaus **200** kann auch Überprüfungen von Verbraucherkrediten und Berechtigungen bereitstellen und dadurch dazu beitragen, dass der Verbraucher keine große Rechnung verursacht, die er nicht bezahlen kann.

[0549] Media Player **104** kann die von ihm erfasste Benutzungsinformation an ein Usage-Clearinghaus **300** übermitteln, das von einem unabhängigen Auditor betrieben wird (es kann sein, dass der Filmproduzent und die Schauspieler darauf bestehen, dass ein Auditor eines unabhängigen Dritten – nicht Disney – diese Funktion ausführt) oder kann zum Beispiel derartige Daten an Disney und/oder Clearinghaus **200** übermitteln – bestimmte Daten können bei Disney verborgen bleiben, wenn dies durch Regeln und Steuermechanismen so festgelegt ist, um die Rechte anderer Teilnehmer der Wertkette zu garantieren, und es kann sein, dass Disney, zum Beispiel aufgrund von VDE-Schutzmechanismen, nicht in der Lage ist, derartige Daten zu identifizieren, zu verändern und/oder zu entfernen. Das Usage-Clearinghaus **300** kann die Benutzungsdaten analysieren und Berichte ausstellen, die angeben, wie oft der Film gezeigt wurde, den Marktanteil, etc., Usage-Clearinghaus **300** kann auch die Information weiter analysieren, um demographische und/oder andere Martkforschungsdaten bereitzustellen. Diese Art von Information kann sehr nützlich für Werbetreibende und Verkäufer sein.

[0550] Disney kann auch ein Rechte- und Berechtigungs-Clearinghaus **400** betreiben. Auch wenn Berechtigungen in diesem Beispiel auf dem optischen Medium verteilt sind, kann das Rechte- und Berechtigungs-Clearinghaus aus verschiedenen Gründen zusätzliche Regelsätze bereitstellen. Zum Beispiel können die auf dem Medium verteilten Regelsätze zu einem bestimmten Datum auslaufen. Rechte- und Berechtigungs-Clearinghaus **400** kann neue Regelsätze anstatt der abgelaufenen ausgeben. Rechte- und Berechtigungs-Clearinghaus **400** kann auch Berechtigungen ausgeben, um einen "Ausverkauf" durchzuführen und/oder um auf eine andere Art und Weise die Preise zu verändern (z. B. um den Preis eines älteren Films zu verringern). Rechte- und Berechtigungs-Clearinghaus **400** kann auch spezielle Berechtigungen (z. B. ein Recht, einen Auszug oder eine Anthologie zu erstellen, das Multi-Media-Entwickler anfordern können, und/oder, zum Beispiel,

die Weiterverkaufsrechte für bestimmte Bilder, wie zum Beispiel ein freigegebenes Bild von Mickey Mouse für das Abdrucken) ausstellen. Disney könnte auch im Voraus einige dieser Berechtigungen ausstellen, so dass das Rechte- und Berechtigungs-Clearinghaus sie automatisch auf Anforderung bereitstellen könnte. Digitale Zertifikate **122** könnten verwendet werden, um mit den Berechtigungen zusammen zu wirken und um dadurch garantieren, dass der Benutzer, der den Regelsatz erhält, auch die Berechtigung hat, ihn zu nutzen.

Beispiel: Das Distributed Commerce Utility **75** kann das Erfassen, Analysieren und Umwidmen von Benutzungsinformation unterstützen

[0551] Vor den in der Patentanmeldung von Ginter et al. offenbarten Erfindungen gab es in der elektronischen Gemeinschaft keine allgemeinen, umnutzbaren, verteilten, Peer-to-Peer-Technologien, die unter anderem effizient und effektiv die Benutzung auf dem lokalen Computer oder der geschützten Verarbeitungsumgebung überwachen und messen könnten. Das Erfassen, Analysieren und Übermitteln von Benutzungsdaten ist für Rechteinhaber und andere Teilnehmer der Verteilungskette sowie für die Infrastruktur des Distributed Commerce Utility **75**, Verbraucher und weitere betroffene Parteien von großer Bedeutung. Das Verstehen dessen, was geschehen ist, kann oft ein grundlegender Faktor sein, mit dem bestimmt werden kann oder der dazu beitragen kann, zu bestimmen, was passieren könnte oder sollte. Zusätzlich kann Benutzungsinformation umgewidmet werden, um eine große Bandbreite von weiteren kommerziellen Aktivitäten, einschließlich Werbungs- und Vermarktungsmodellen, zu unterstützen.

[0552] Man nehme an, dass einer oder mehr Verbraucher in jeder von mehreren verschiedenen Unternehmen Datengeräte **100** besitzen, wie etwa Personal-Computer in diesem Beispiel mit geschützten VDE-Verarbeitungsumgebungen (PPEs) **154** wie in Ginter et al beschrieben. Weiter sei angenommen, dass über einen bestimmten Zeitraum hinweg, wie etwa einen Monat in diesem Beispiel, dieses VDE detaillierte Benutzungsinformation aufgenommen hat und diese Information in der verschlüsselten Datenbank auf jeder Festplatte auf jedem Computer, der eine logische Erweiterung darstellt, sowie unter der Kontrolle der PPE jedes Verbrauchers gespeichert hat. Diese Verbraucher haben verschiedene Zusammenstellungen von Informationen und Unterhaltung von im Allgemeinen voneinander verschiedenen Quellen eingekauft. Jede Ebene der VDE verfolgt die Benutzungsinformation gemäß den mit dem Inhalt assoziierten Regeln und/oder mit dem Dienst, der eingekauft oder in anderer Weise verwendet wurde.

[0553] Am oder kurz nach dem Ersten jeden Monats und/oder jeder anderen erforderlichen (oder, wenn dies unterstützt wird, erlaubten) Zeitspanne, übermittelt jede VDE-Ebene die Benutzungsprotokolle an das Benutzungs-Clearinghaus **300** gemäß den entsprechenden dem jedem digitalen Eigentum assoziierten Regeln, die sie während des vorhergehenden Monats verwendet haben. Daraufhin stellt das Usage-Clearinghaus **300** jedem Rechteinhaber Berichte bezüglich der Benutzung eines Eigentums während des vorangehenden Monats oder einer anderen Zeitspanne bereit (z.B. täglich, wöchentlich, vierteljährlich, jährlich, etc.).

[0554] In einem Beispiel enthalten diese Protokolle Daten, die sowohl den Einzelverbraucher als auch das Unternehmen, das sie beschäftigt identifizieren. In einem weiteren Beispiel enthalten die Protokolle detaillierte Benutzungsdaten, jedoch wurden die Erkennungsdaten der Einzelverbraucher von dem Benutzungs-Clearinghaus **300** entfernt. Alternativ könnten sowohl die Erkennungsdaten von Einzelpersonen als auch von Unternehmen entfernt werden. Stattdessen kann die Benutzungsinformation nach einer beliebigen oder mehr bestimmten Klassen aggregiert werden, wie etwa nach Gewerbe, geographischer Lage und/oder Land und/oder jede beliebige weitere nützliche Klasse.

[0555] In einem weiteren nützlichen Beispiel kann es sein, dass ein bestimmtes Unternehmen oder ein Einzelverbraucher der VDE nicht erlaubt haben, Erkennungsdaten von ihren Datengeräten an das Usage-Clearinghaus **300** zu übertragen (was natürlich abhängig davon ist, ob dieses Recht durch gültige Regeln und Steuermechanismen verfügbar ist). Der Benutzer kann VDE-Regeln eingerichtet haben, welche die Offenbarung derartiger Kennungsdaten verbieten. In einem weiteren Beispiel kann der Benutzer die in der Ginter et al. Patentschrift beschriebenen Verhandlungsmechanismen verwenden, um zusätzliche Geheimhaltungs- und Vertraulichkeitsebenen zu verhandeln, die sich von denen, die in den verschiedenen Regelsätzen erforderlich sind unterscheiden und die mit den Daten, die eingekauft und oder auf andere Weise verknüpft sind, das heißt, der elektronische Verhandlungsprozess erzeugt einen modifizierten oder neuen Satz von Regeln und Steuermechanismen, in welchen die zusätzlichen Geheimhaltungs- und Vertraulichkeitsebenen repräsentiert sind. In noch einem weiteren Beispiel können ein Rechteinhaber, das Rechte- und Berechtigungs-Clearinghaus **400** oder das Usage-Clearinghaus **300** oder eine andere Partei dieselben Verhandlungsmechanismen verwendet haben, um durch die Benutzung von VDE-Sätzen von Regeln und Steuermechanismen andere Ebenen der Geheimhaltung und Vertraulichkeit zu verhandeln.

[0556] Wie in Fig. 11 und Fig. 33-Fig. 39 veranschaulicht, können die Usage-Clearinghaus-Funktionen, welche identifizierende Daten entfernen, Daten

aggregieren können, Protokolle erstellen können und/oder diese an Rechteinhaber und andere betroffene Parteien übertragen können, an einem oder mehr logischen oder physikalischen Orten vorliegen. Zum Beispiel kann ein verteiltes Usage-Clearinghaus **300**, das auf dem lokalen Computer ausgeführt wird (oder einem anderen Datengerät) jedes dieser Usage-Clearinghaus-Funktionen ausführen. Eines oder mehr Usage-Clearinghäuser können innerhalb eines bestimmten Unternehmens oder innerhalb eines bestimmten Zusammenschlusses von Unternehmen vorhanden sein, die eine vertikale Industrie, eine Handelsgruppe oder eine Unternehmensgruppe („keiretsu") umfasst. In ähnlicher Weise können diese Funktionen des Usage-Clearinghauses durch Usage-Clearinghäuser innerhalb jedes Landes oder einer anderen Gerichtsbarkeit oder innerhalb jeder beliebigen anderen Klasse und/oder geographischen Variable durchgeführt werden.

[0557] Usage-Clearinghaus **300** kann auch Originaldaten, aggregierte Daten und/oder individualisierte Protokolle für Rechteinhaber, Teilnehmer der Verteilungskette und/oder andere betroffene Parteien bereitstellen. Diese Parteien schließen ein: Zum Beispiel Ersteller von Inhalten, Herausgeber, Repackager, Umwidmer, Werbeagenturen und deren Kunden, Wirtschaftsverbände, Marktforschungs- und Beratungsunternehmen, Büros für Auflagenkontrolle und Einschaltquotenmessung, die Verkaufs-, Marketing und Werbungsfunktionen von Unternehmen mit einem Interesse auf einem oder mehr Märkten sowie Regierungsbehörden.

[0558] In einem weiteren Beispiel kann das Usage-Clearinghaus **300** auch Daten an Werbetreibende verkaufen, die einen Kontakt mit bestimmten Anzeigen und/oder Klassen von Anzeigen durch Einzelpersonen, Verbraucher innerhalb eines Unternehmens und/oder Gruppe von Unternehmen, Märkten und/oder anderen Analysegruppierungen und Kategorien anzeigen.

Beispiel: Sichere Verzeichnisdienst schützen Vertraulichkeit und Geheimhaltung

[0559] Private und geschäftliche Vertraulichkeit und Geheimhaltung sind oft essenzielle Aspekte des modernen Lebens. Es kann sein, dass Einzelpersonen nicht möchten, dass andere wissen, mit wem sie assoziiert sind. In vielen geschäftlichen Bereichen kann es sein, dass Firmen nicht zeigen möchten, dass sie ein Interesse an der Kommunikation, Interaktion oder dem Abschließen von Geschäften mit anderen Parteien haben. Heutzutage ist es zum Beispiel im Internet möglich, dass Personen mit einer bestimmten Art von Zugriff die Art von Anfragen zwischen einer bestimmten Person und einem Verzeichnisdienst bestimmen können. Derartige Daten können wichtige Hinweise auf bestehende oder bevorstehende Geschäftsvereinbarungen geben, die noch nicht öffentlich bekannt sind, wie zum Beispiel eine Fusion oder eine Übernahme.

[0560] Sichere VDE-Container stellen eine Basis für sichere Verzeichnisdienste **600** bereit, in denen Vertraulichkeit und Geheimhaltung geschützt sind. In einem Beispiel möchte der Corporation Counsel in einem Fortune **100** Unternehmen die E-Mail-Adresse des Investmentbankers des Unternehmens, das gerade eine Übernahme durchführt, erhalten – jedoch ohne dessen Interessen jemand anderem mitzuteilen. Der Anwalt schickt eine Anfrage in einem sicheren VDE-Container an den sicheren Verzeichnisdienst **600** mit dem Namen und dem Unternehmen der Person, die er kontaktieren möchte. Der sichere Verzeichnisdienst sendet dann die Antwort in einem weiteren sicheren VDE-Container zurück an den Anwalt. Sowohl die Anfrage als auch die Antwort können die von der zertifizierenden Behörde ausgegebenen Zertifikate anwenden, die sowohl den Anwalt als auch den sicheren Verzeichnisdienst **600** authentifizieren. Bezahlung der Anfrage kann in dem Finanz-Clearinghaus **200** abgewickelt werden, das die Bezahlung in dem Konto des Anbieters des sicheren Verzeichnisdienstes **600** niederlegt, während es das Konto des Unternehmens belastet, das den Anwalt beschäftigt.

[0561] Da drei Transaktionen unter Verwendung von VDE und sicheren VDE-Containern durchgeführt werden, erfahren Beobachter des Datenverkehrs nicht mehr als die Tatsache, dass diese Parteien miteinander kommunizieren. Sicherheitsanalysten haben Techniken zur „Datenverkehrsanalyse" entwickelt, bei denen die Häufigkeit des Datenverkehrs zwischen zwei oder mehr Parteien beobachtet wird und Veränderungen in der Häufigkeit der Kommunikation mit anderen Daten in Verbindung stehen, um Rückschlüsse auf den Inhalt und/oder Zweck dieses Datenverkehrs zu ziehen.

[0562] Unter Verwendung von VDE und sicheren VDE-Containern ist es mit jedoch leicht erhöhtem Kostenaufwand möglich, eine Datenverkehrsanalyse zu abzuwehren. In diesem einen Beispiel könnte das Unternehmen einen VDE-Container an den sicheren Verzeichnisdienst **600** mit einer leeren oder „ungültigen" Anfrage senden, der in der Durchschnittsmenge der abgelaufenen Zeit eine zurückgesendete Nachricht in einem VDE-Container mit einer „ungültigen" Antwort erzeugt. Die VDE-Ebene auf dem Computer des Anwalts könnte eine Bezahlungstransaktion erzeugen, die für das Finanz-Clearinghaus bestimmt ist, würde jedoch diese Zahlungsaufzeichnungen mit anderen aggregieren, um Übereinstimmungen zwischen den Mustern der Abfragen und Zahlungen zu eliminieren. Auch wenn dieses Verfahren des Verwendens von VDE und sicheren VDE-Containern für das Verhindern von Angriffen zur Datenverkehrsana-

lyse von einem kommerziellen Standpunkt gesehen ineffizient ist, kann es im Prinzip zwischen mehreren Parteien verwendet werden, um die Muster des Datenverkehrs zwischen ihnen zu verbergen, während die sicheren, vertrauenswürdigen, effizienten, verteilten Transaktionseigenschaften, die in der Ginter et al. – Anmeldung offenbart wurden, genutzt werden.

Beispiel: Kooperation zwischen Clearinghäusern, die innerhalb und außerhalb einer Organisation liegen

[0563] Die verschiedenen Commerce Utility Systeme **90** können variabel verteilt werden und in variablen Kombinationen (wie in Fig. 2A-Fig. 2E und Fig. 3A-Fig. 3C veranschaulicht). In einem in Fig. 65 gezeigten Beispiel war es für ein American Fortune **100** Unternehmen **1070**, das Geschäfte in mehreren Ländern betreibt (z. B. den Vereinigten Staaten, Japan und Europa) und innerhalb vieler dieser Länder an vielen Orten innerhalb jedes Landes mehrere Standorte hat, wünschenswert, das verteilte VDE-Commerce Utility **75** international zu verteilen.

[0564] Um die Effizienz des Einkaufs von externer Information zu erhöhen und um seinen Einfluss mit Datenanbietern zu maximieren, hat das Unternehmen **1070** es vorgezogen, mit mehreren Anbietern Vereinbarungen zu verhandeln, die alle Einkäufe so behandeln, als wären sie innerhalb der Vereinigten Staaten und in US-Dollar getätigt worden. In diesem Beispiel unterhält das Unternehmen **1070** sein eigenes globales Intranet **1072**. Intranet **1072** verbindet Unternehmenshauptsitz **1074HQ** (hier als in den Vereinigten Staaten ansässig gezeigt) mit den elektronischen Geräten der Angestellten des Unternehmen in den Vereinigten Staaten **1074US(1)**, ..., **1074US(N)**, mit elektronischen Geräten der Angestellten in Japan **1074JP(1)**, ..., **1074JP(N)**, und elektronischen Geräten der Angestellten in Europa **1074EU(1)**, ... **1074EU(N)**. Intranet **1072** erlaubt allen Angestellten **1074**, miteinander zu kommunizieren. VDE-basierte Transaktionen zwischen dem Unternehmen **1070** und dessen Datenlieferanten werden ebenfalls durch ein beliebiges Gateway des Unternehmens in den Vereinigten Staaten an das Internet geleitet.

[0565] Um effektive Verwaltungs- und Unterstützungsdienste anzubieten, hat das Unternehmen **1070** in jedem Land wenigstens ein verteiltes Finanz-Clearinghaus **200** eingerichtet sowie wenigstens ein verteiltes Usage-Clearinghaus **300**. Zum Beispiel kann Unternehmen **1070** ein Finanz-Clearinghaus **200A** und ein Usage-Clearinghaus **300A** in den Vereinigten Staaten betreiben, ein Finanz-Clearinghaus **200B** und ein Usage-Clearinghaus **300B** in Japan und ein Finanz-Clearinghaus **2000** und ein Usage-Clearinghaus **3000** in Westeuropa. In Ländern mit vielen Standorten und innerhalb der Vereinigten Staaten können mehrere dieser verteilten Clearinghäuser existieren. Zusätzlich zu dem Verhandeln von Vereinbarungen mit Datenanbietern kann das Unternehmen **1070** auch verhandelte Vereinbarungen mit einem großen kommerziellen Usage-Clearinghaus **300** und mit einem größeren Finanz-Clearinghaus **200** führen. Diese zentralisierten Clearinghäuser könnten an jedem beliebigen Ort ansässig sein und können mit Unternehmen **1070** über das Internet und das Unternehmensintranet **1072** kommunizieren. Keines dieser Clearinghäuser **200**, **300** ist mit dem Unternehmen anders verbunden als über diese Geschäftsvereinbarung. Jedes verteilte Clearinghaus innerhalb des Unternehmens **1070** wird unter der gleichzeitigen Erlaubnis sowohl des Unternehmens als auch den externen Clearinghäusern, mit denen das Unternehmen eine Geschäftsvereinbarung hat, betrieben.

[0566] In diesem einen Beispiel erwirbt ein Produktmarketingmanager **1074JP(1),** der bei diesem Unternehmen **1070** in Japan angestellt ist, einen Marktforschungsbericht **166** von einem amerikanischen Verteiler **1076**. Der Bericht und assoziierte Regeln werden von dem amerikanischen Verteiler **1076** in einem sicheren VDE-Container **152a** an diesen Angestellten **1074JP(1)** gesendet. Die VDE-Ebene auf dem Gerät des Managers **1074JP(1)** verfolgt die Benutzung und die dem Informationsanbieter geschuldete Bezahlung weiter. In regelmäßigen Zeitabständen werden diese Audit-Aufzeichnungen in sicheren VDE-Containern **1052b**, **1052c** an das verteilte Usage-Clearinghaus (privates Usage-Clearinghaus) **300B** und an das interne Finanz-Clearinghaus **200B** übertragen – von denen beide in Japan in dem internen, privaten Unternehmensnetzwerk (oder Intranet) **1072** ansässig sind. Von Zeit zu Zeit und gemäß den mit dem eingekauften Inhalt assoziierten VDE-Regeln entfernt das private Usage-Clearinghaus **300B** individuelle identifizierende Information gemäß den VDE-Regeln und Steuermechanismen, welche die Prozesse der geschützten Verarbeitungsumgebung steuern und versendet die Audit-Aufzeichnungen **302(3)** in einem sicheren VDE-Container an das externe, kommerzielle Usage-Clearinghaus **300**. Jedes interne verteilte Usage-Clearinghaus des Unternehmens **300A**, **300B**, **300C** sendet periodischen Datenverkehr in sicheren VDE-Containern **152** an das kommerzielle Usage-Clearinghaus **300**. Daraufhin erstellt und verkauft, lizenziert und/oder verteilt in anderer Weise das Usage-Clearinghaus der obersten Ebene **300**, Aufzeichnungen an andere Parteien (z. B. dritte Parteien mit einem kommerziellen Interesse, die Information zu erhalten) in denen die Identitäten von Einzelpersonen entfernt wurden und bei denen in vielen Fällen auch Unternehmensnamen, gemäß den VDE-Regeln und Steuermechanismen entfernt wurden.

[0567] Von Zeit zu Zeit und gemäß den mit dem eingekauften Inhalt **166** assoziierten VDE-Regeln **188a** werden auch Kopien der gesamten Benutzungspro-

tokolle (mit Daten zur Identifikation der Angestellten) an das oberste Usage-Clearinghaus **300HQ** des Unternehmens (die an Unternehmenshauptsitzen ansässig sein können), wie auch Audit-Aufzeichnungen von sämtlichen verteilten Usage-Clearinghäusern **300A**, **300B**, **300C** gesendet. Diese werden dann aggregiert und für eine weitere Analyse, Berichterstattung und Auditing zusammengestellt.

[0568] Die internen, verteilten Finanz-Clearinghäuser **200A**, **200B**, **200C** erhalten auch Audit-Aufzeichnungen **302** in sicheren VDE-Containern **152** gemäß den VDE-Regelsätzen für die eingekauften Daten von jeder der geschützten VDE-Verarbeitungsumgebungen **1074**, die ihnen Daten übermitteln. Jedes interne Finanz-Clearinghaus **200A**, **200B**, **200C** aggregiert die Zahlungen und sendet von Zeit zu Zeit einen sicheren VDE-Container **152** mit Audit-Aufzeichnungen **302**, welche die aggregierten Summen, die an den Informationsanbieter als ein Ergebnis der Transaktion überwiesen werden sollen, angeben. Das Unternehmen kann auch Update-Information bezüglich der Konten von denen die Gelder des Unternehmens überweisen werden sollen und/oder die Konten der Anbieter, die derartige Gelder erhalten sollen, bereitstellen. Daraufhin schließt das externe Finanz-Clearinghaus **200** der obersten Ebene diese Zahlungstransaktionen ab und sendet Audit-Aufzeichnungen an das Unternehmen **1070** sowie an die Informationsanbieter, die die Zahlungstransaktionen bestätigen zurück. In der bevorzugten Ausführungsform werden diese Aktivitäten sicher unter der Kontrolle verteilter VDE-Knoten ausgeführt und werden wenigstens teilweise durch die Verwendung von VDE-Containern und Verarbeitungs- und Steuerketten, die Prozessabfolgen mit einer Vielzahl von Knoten und Parteien verwalten, sicher durchgeführt. Als ein alternatives Beispiel wird die Berechnung des Zahlungsbetrages und der Abschluss der Zahlungstransaktionen bei dem externen obersten Finanz-Clearinghaus **200** auf Grundlage von dem Usage-Clearinghaus **300** erhaltener Benutzungsinformation (natürlich hat das Finanz-Clearinghaus diese Information bereits erhalten, wenn Benutzungs-Clearinghaus **300** und Finanz-Clearinghaus **200** zur selben Partei gehören). Das externe und interne Finanz-Clearinghaus könnten dann in diesem Beispiel die Zahlungsdaten vergleichen.

[0569] Dieses Beispiel hängt nicht davon ab, in welchem Ausmaß Verwaltungs- und Unterstützungsdienste verteilt sind. In einem zugehörigen Beispiel könnten die Funktionen der Usage- und Finanz-Clearinghäuser an jede VDE-fähige geschützte Verarbeitungsumgebung **1074** verteilt werden, wie in Fig. 2A-Fig. 2E und Fig. 3A-Fig. 3C veranschaulicht. In diesem Beispiel könnte jede geschützte Verarbeitungsumgebung **1074** direkt den externen Clearinghäusern **200**, **300**, den verteilten externen Clearinghäusern und/oder internen Clearinghausfunktionen, die anders als oben beschrieben verteilt sind, zum Beispiel nach Kontinent (Nordamerika, Süd- und Mittelamerika, Australien, Europa, etc.) anstatt nach dem Unternehmenssitz **1070** des Unternehmens, Bericht erstatten.

[0570] In einem weiteren Beispiel stellen die Unternehmenshauptquartiere **1074HQ** und deren assoziierte Hauptquartier-basierte Clearinghäuser **200HQ**, **300HQ** ein zentralisiertes Clearinghaussystem bereit, das sämtliche Benutzungs- und Finanzdaten durchlaufen müssen. In diesem speziellen, zentralisierteren Beispiel berichten sämtliche benutzerseitige Geräte **1074** über Intranet **1072** in sicheren Containern **152** ihre Benutzungs- und Finanztransaktionen an Hauptquartier-basierte Clearinghäuser **200HQ**, **300HQ**. Finanz-Clearinghaus des Unternehmenshauptsitzes **200HQ** kann eine direkte Schnittstelle mit VDE-kompatiblen allgemeinen Zahlungssystemen sein, die direkt die Verwendung der VDE-Verarbeitungs- und Steuerungskette für das Gewährleisten der Durchführung einer automatisierten, sicheren Ausführung finanzieller Transaktionen gemäß den Regeln und Steuermechanismen, welche die zur Zahlung gehörige Variablen wie etwa Zahlungsbeträge, Parteien, Orte, Zeitplanungen und/oder weitere Bedingungen leiten, unterstützen. Diese Hauptsitz-basierten Clearinghäuser **200HQ**, **300HQ** (die als ein einzelnes integriertes Commerce Utility System funktionieren können) können wiederum geeignete aggregierte und/oder weitere Prüfketten- und/oder Zahlungsdaten an die einzelnen Clearinghäuser **200A**, **200B**, **200C**, **300A**, **300B**, **300C** weiterleiten. Auch wenn diese Anordnung weniger effizient ist als das weniger hierarchische, oben beschriebene Beispiel, kann sie für große Unternehmen attraktiv sein, wenn diese wünschen, eine zentralisierte Kontrolle der Benutzungs- und Finanzinformation durch ihre Funktion als zentraler Administrator für die Bereitstellung eines Kredits und/oder elektronischer Währung an verteilte interne Finanz-Clearinghäuser sowie durch das effektive Durchführen einer internen Erfassung von Transaktionsdaten, auszuüben.

Beispiel: Transaktionsbehörden können innerhalb und zwischen Organisationen verwendet werden.

[0571] Fig. 66 zeigt eine beispielhafte Verwendung der Transaktionsbehörde **700** für inter- und intraorganisatorischen Datenverkehr. Fig. 66 zeigt eine Organisation A (linke Seite der Zeichnung), die ein „Intranet" besitzt (ein privates Datennetzwerk innerhalb einer bestimmten Organisation) **5100(A)**. Intranet **5100(A)** kann zum Beispiel ein lokales und/oder großflächiges Netzwerk sein. Benutzerseitige Geräte **100(A)(1)**, ..., **100(A)(N)** (zum Beispiel Angestellte von Organisation A) können über Intranet **5100(A)** miteinander kommunizieren.

[0572] Fig. 66 zeigt eine weitere Organisation B, die ihr eigenes Intranet **5100(B)**, benutzerseitige elektronische Geräte **100(B)(1)**, ... **100(B)(N)**, sowie eine private Transaktionsbehörde **700(B)** besitzen kann. Zusätzlich zeigt Fig. 66 ein öffentliches Datennetzwerk **5104** (wie etwa zum Beispiel das Internet) sowie eine öffentliche Transaktionsbehörde **700(C)**. Fig. 66 zeigt, dass in diesem Beispiel Organisationen A und B mit dem Rest der Welt über die vertrauenswürdige Transaktionsbehörde **700(A)**, **700(B)** kommunizieren (die gegebenenfalls auch „Gateways", „Firewalls" und weitere assoziierte sichere Datenübertragungskomponenten einschließen). In weiteren Beispiel muss vertrauenswürdige Transaktionsbehörde **700(A)**, **700(B)** nicht die eigentliche „Gateway" und „Firewall" zu/von Internet **5104** sein, könnte jedoch stattdessen komplett innerhalb der jeweiligen Organisationen A, B arbeiten, während sie möglicherweise elektronische Container **302** für die Übertragung über Internet **5104** erzeugt.

[0573] In diesem Beispiel haben die geschützten Benutzerverarbeitungsumgebungen der Organisation A **100(A)(1)**, ... **100(A)(N)** jeweils eine Ebene einer geschützten VDE-Verarbeitungsumgebung und können miteinander über Intranet **5100(A)** über sichere elektronische Container **302** kommunizieren. In ähnlicher Weise haben die elektronischen benutzerseitigen Geräte **100(B)(1)**, ... **100(B)(N)** der Organisation A eine Ebene einer geschützten VDE-Verarbeitungsumgebung und können miteinander über Intranet **5100(B)** über sichere elektronische Container **302** kommunizieren. Zusätzlich können Organisation A und Organisation B miteinander über Internet **5104** über sichere elektronische Container **302** miteinander kommunizieren.

[0574] Die private vertrauenswürdige Transaktionsbehörde **700(A)** der Organisation A kann verwendet werden, um den internen Datenverkehr und die Prozesse der Organisation A zu vereinfachen. Private vertrauenswürdige Transaktionsbehörde **700(A)** kann zum Beispiel verwendet werden, um Produkte sorgfältig zu verfolgen, die innerhalb Organisation A von einem Benutzer zu einem anderen versendet werden. Die öffentliche Transaktionsbehörde **700(C)** kann währenddessen verwendet werden um zwischen Organisation A und Organisation B zu koordinieren, ohne zum Beispiel der einen Organisation vertrauliche Information der anderen zu enthüllen. Untenstehend finden sich detailliertere Beispiele dafür, wie die Anordnung in Fig. 66 in vorteilhafter Weise verwendet werden könnte, um Geschäftstransaktionen durchzuführen.

[0575] Es sei angenommen, dass ein vertrauliches Memo von Benutzern **100(A)(1)**, **100(A)(3)** und **100(A)(5)** genehmigt wird (die jeweils das Memo überarbeiten können), bevor sie an Benutzer **100(A)(2)**, **100(A)(7)**-**100(A)(10)** und **100(A)(12)** (von denen keiner das Memo verändern kann) verteilt werden, mit Kopien, die an Benutzer **100(A)(1)**, **100(A)(3)** und **100(A)(5)** (die ebenfalls das Memo nicht ändern können, nachdem alle drei von ihnen darauf unterschrieben haben) und an keinen sonst gesendet werden. Private Transaktionsbehörde **700(A)** kann einen Regelsatz unterhalten, der diese Anforderungen festlegt. Transaktionsbehörde **700(A)** kann folgendes tun:

- das Memo (in sicheren Containern) als Rundschreiben an jeden Benutzer **100(A)(1)**, **100(A)(3)** und **100(A)(5)** zur Bestätigung senden.
- Wenn einer dieser Benutzer das Memo verändert, dann kann die Transaktionsbehörde **700(A)** das überarbeitete Memo für zusätzliche Kommentare und Korrekturen an die anderen beiden senden.
- Wenn alle drei Benutzer **100(A)(1)**, **100(A)(3)** und **100(A)(5)** das Memo bestätigt haben, dann kann Transaktionsbehörde **700(A)** berechtigt werden, jede ihrer digitalen und/oder handschriftlichen Signaturen oder Initialen auf das Memo zu setzen, es in einen oder mehr sichere Container packen und festlegen, dass es nur lesbar ist und nur von Benutzern **100(A)(1)**-**100(A)(3)**, **100(A)(5)**, **100(A)(7)** -**100(A)(10)** und **100(A)(12)** gelesen werden kann.
- Transaktionsbehörde **700(A)** kann dann eine Kopie des Memos in einem Container an jeden Benutzer senden oder könnte bewirken, dass derselbe Container von einem Benutzer zum nächsten weitergesendet wird.
- Die Transaktionsbehörde **700** kann die elektronische Steuerung dazu veranlassen, einen sicheren Audit durchzuführen, über die sich zurückverfolgen lässt, wo der Container war, wer ihn geöffnet hat, wer Zugriff auf das Memo hatte, das er enthält, und wann Transaktionsbehörde **700(A)** dadurch die persönliche Verantwortbarkeit erhöhen könnte, indem sie beweist ob eine bestimmte Person ein bestimmtes Dokument gesehen hat, wann dies geschehen ist und wie lange.

[0576] Das Intranet **5104** von Organisation A kann auch verwendet werden, um in höchstem Maße vertrauliche Designbeschreibungen auszutauschen und/oder zu verteilen. Transaktionsbehörde **700(A)** kann zum Beispiel ein digitales Formular, ein detailliertes Protokoll darüber, wer die Designbeschreibungen unterzeichnet und freigegeben hat – und sichert so die persönliche Verantwortbarkeit und stellt ein hohes Maß an Effizienz bereit.

[0577] Wie oben erwähnt könnte private Transaktionsbehörden **700(A)**, **700(B)** auch eine „Firewall"-Funktion bereitstellen, um zu verhindern, dass vertrauliche Information die jeweiligen Organisationen A, B verlässt. Man stelle sich zum Beispiel vor, dass Organisation A ein Unternehmen ist, das integrierte Schaltkreise entwirft und dass Organisation B

ein Unternehmen ist, das integrierte Schaltkreise herstellt. Organisation A entwickelt und entwirft die Schaltkreise auf einem Chip und stellt ein „Tape out" her, das sie an Organisation B sendet. Organisation B stellt basierend auf dem „Tape out" einen integrierten Schaltkreis her und liefert Chips an Organisation A.

[0578] Transaktionsbehörde **700** kann verwendet werden, um die darüber stehende Geschäftstransaktion zu vereinfachen und schützt gleichzeitig die Vertraulichkeit innerhalb jeder Organisation A und B. Zum Beispiel:

- kann die private Transaktionsbehörde **700(A)** der Organisation A einen Gesamtentwicklungsaufwand von Designbeschreibungen innerhalb Organisation A überwachen. Sämtlicher Datenverkehr geschieht in sicheren Containern **302** in Organisation A Intranet **5100(A)**, um die Vertraulichkeit zu gewährleisten. Transaktionsbehörde **700(A)** kann ein sicheres Archiv mit älteren Dokumenten zum Design unterhalten, mit in der Entwicklung befindlichen Designs und mit Beschreibungen des Fortschritts der Designbeschreibung.
- kann die private Transaktionsbehörde **700(A)** der Organisation A eine abschließende Entwicklung einer Designbeschreibung verwalten und so sicherstellen, dass alle Vorschriften für das Abschließen der Designbeschreibungen befolgt werden.
- Wenn die Designbeschreibungen abgeschlossen ist, kann Transaktionsbehörde **700(A)** sie innerhalb von sicheren Containern **152** an die Personen innerhalb von Organisation A weiterreichen, die sie unterzeichnen und freigeben müssen. Ihre jeweiligen Geräte **100(A)(1)**, **100(A)(k)** können digitale Signaturen anhängen und/oder implementieren, handschriftliche Unterschriften, Siegel und/oder Fingerabdrücke wie oben beschrieben, um die Abzeichnung der Beschreibung anzuzeigen.
- Sobald mitgeteilt wurde, dass die Spezifikation von den jeweiligen Personen unterzeichnet und freigegeben wurde, kann Transaktionsbehörde **700(A)** sie über Internet **1104** in einem sicheren Container **302** an die öffentliche Transaktionsbehörde **700(C)** senden. Öffentliche Transaktionsbehörde **700(C)** kann eine kommerzielle Transaktionsbehörde sein, die von Organisationen A und B verwendet wird, um eine Verbindung zwischen ihnen zu bewirken. Die private Transaktionsbehörde **700(A)** der Organisation A kann sämtliche Daten, die sie an die öffentliche Transaktionsbehörde **700(C)** sendet, filtern (oder schützen), um sicherzustellen, dass Organisation B nur Zugriff auf die Daten erhält, die für sie bestimmt sind. Zum Beispiel kann private Transaktionsbehörde **700(A)** zusätzliche elektronische Steuerungsmechanismen innerhalb des Containers einführen, um zu verhindern, dass Organisation B Zugriff auf detaillierte Auditdaten bekommt, die zeigen, wo die Spezifikation innerhalb von Organisation A war.
- Die öffentliche Transaktionsbehörde **700(C)** kann als unabhängige, vertrauenswürdige dritte Partei wirken, die die Designbeschreibung für einen späteren Nachweis, dass Organisation A sie an einem bestimmten Datum und zu einer bestimmten Zeit gemäß dem Vertrag geliefert hat beglaubigt und/oder zertifiziert.
- Öffentliche Transaktionsbehörde **700(C)** könnte dann die Designbeschreibung (nach wie vor in einem sicheren Container) über das Internet **5104** an die private Transaktionsbehörde **700(B)** der Organisation B senden.
- Die private Transaktionsbehörde **700(B)** der Organisation B könnte automatisch eine Kopie der Designspezifikation über das Intranet **5100(B)** der Organisation B an die jeweiligen Benutzer **100(B)(1)**,**100(B)(N)** innerhalb von Organisation B senden. Keiner außerhalb von Organisation B muss erfahren, wer eine Kopie der Beschreibung erhalten hat. Andererseits könnte die Transaktionsbehörde **700(A)** der Organisation A, falls dies gewünscht wird, elektronische Steuerungen einschließen, die den Zugriff auf einige wenige Ingenieure innerhalb von Organisation B beschränken, und diese sicheren Steuerungen würden mit in Organisation B gebracht und von elektronischen Geräten **100(B)(1)**, ..., **100(B)(N)** sicher ausgeführt.

[0579] Die Transaktionsbehörde **700(B)** der Organisation B könnte die Chipherstellung durchführen und sicherstellen dass alle Schritte und Vorschriften die für das Herstellen von Chips gemäß der Designbeschreibung der Organisation A erforderlich sind, ausgeführt werden.

Beispiel: Die Transaktionsbehörde kann den internationalen Handel vereinfachen

[0580] Fig. 67 zeigt eine beispielhafte Verwendung der Transaktionsbehörde **700** für den internationalen Handel. In diesem speziellen Beispiel koordiniert eine Transaktionsbehörde **700** eine komplexe multi-nationale Transaktion zwischen Unternehmen **1106A**, **1106B** und **1106C**, die in ihren jeweiligen Ländern ansässig sind (z. B. die Vereinigten Staaten, Australien und Europa). Unternehmen **1106A** hat seine eigene Bank **1108A** und Anwälte **1110A**. In gleicher Weise hat Unternehmen **1106B** seine eigene Bank **1108B** und Anwälte **1110B**, und Unternehmen **1106C** hat seine eigene Bank **1108C** und Anwälte **1110C**.

[0581] Dei Transaktionsbehörde **700** kann dabei helfen, Vereinbarungen zwischen den internationalen Parteien zu erreichen, zum Beispiel, indem sie Angebote und Gegenangebote in sicheren Containern zu-

rück- und weiterleitet und die Techniken für das Erstellen eines Vertrags, die oben beschrieben wurden, verwendet, um einige oder alle Geschäftsbedingungen durchzusetzen und eine Nichtrückweisbarkeit bereitzustellen. Sobald ein Vertrag zustande gekommen ist, kann Transaktionsbehörde **700** einen übergeordneten Satz von Regeln und Steuermechanismen unterhalten, der die Bedingungen festlegt, die erfüllt werden müssen, um die Transaktion abzuschließen – und kann somit Konsequenzen für verschiedene Ereignisse festlegen. Alternativ kann die Rolle der Transaktionsbehörde virtuell sein, sobald der Vertrag zustande gekommen ist, insbesondere bei einfacheren Modellen, das heißt, dass die Regeln und Steuermechanismen der Wertkette von VDE-Containern transportiert werden können, deren Regeln und Steuermechanismen als ganzes sämtliche Prozesse und Bedingungen festlegen können, die erfüllt werden müssen, einschließlich der Reihenfolge, in der sie angewendet werden. Regeln und Steuermechanismen, die von einer Transaktionsbehörde **700** bereitgestellt wurden, können internationalen Gesetzen Rechnung tragen, indem verschiedene Regeln für verschiedene Länder angewendet werden. Die Regeln können verschiedene Import- und Exportvorschriften und -einschränkungen einbeziehen, internationale Steuerverträge zwischen Ländern, sie können Routing- und Einreichungsvorschriften für Kunden, die im Voraus oder währenddessen geschehen müssen, festlegen, seriöse Währungstransaktionsbehörden identifizieren, beim Einreichen von Verträgen oder bestimmten Vorschriften in Verträgen bei den jeweiligen nationalen und internationalen Behörden helfen, sie können unterstützen beim Einrichten von Übersetzungsdiensten für Vertragsvorschriften (insbesondere Standardvorschriften und Bedingungen), Unterschiede bei den Vorschriften und Formaten von internationalen zertifizierenden Behörden verwalten, gesellschaftliche Regulierungen die von Regierungsbehörden vorgeschrieben werden, auferlegen, und Steuern von Regierungsbehörden einziehen, wie etwa Steuern sowohl für nationale als auch für regionale Regierungsbehörden, etc. Transaktionsbehörde **700** kann zwischen den verschiedenen internationalen Parteien vermitteln und dabei sichere elektronische Container verwenden und kann sicher verschiedene, von den internationalen Parteien bereitgestellte Ereignismitteilungen validieren und authentifizieren.

Beispiel: Verteilte Transaktionsbehörden

[0582] Komplexe Geschäftsinteraktionen unter der Kontrolle einer Transaktionsbehörde **700** können auch innerhalb und zwischen Organisationen und/oder Gerichtsbarkeiten verteilt werden. Man stelle sich vor, dass eine komplexe internationale Immobilientransaktion die Teilnahme von verschiedenen Stellen innerhalb der kaufenden und der verkaufenden Unternehmen, sowie mehrere Finanzinstitutionen, Versicherungsunternehmen und Anwaltkanzleien, und möglicherweise Regierungsbehörden in mehreren Ländern erfordert. Ferner stelle man sich vor, dass jede der Parteien als Organisation oder Einzelperson der Transaktion Computer besitzt, die VDE-fähig sind, und dass innerhalb jeder Organisation oder Behörde wenigstens eine verteilte Transaktionsbehörde vorhanden ist, die unter der Führung einer obersten Transaktionsbehörde **700** Dienste für diese Immobilientransaktion durchführt.

[0583] In diesem einen Beispiel hat jede der Parteien der Immobilientransaktion Handelsregeln und Parameter aufgestellt, die ihre Geschäftsbeziehungen in Form von VDE-Regeln und Steuermechanismen repräsentieren, welche die Rolle jeder Partei in der Gesamttransaktion definieren. Zum Beispiel muss das Versicherungsunternehmen den Besitz zu einem bestimmten Betrag und zu Kosten versichern, die der Käufer akzeptabel findet und die auch von dem/den Hypothekengeber/n bewilligt werden. Man stelle sich auch vor, dass diese VDE-Regeln und Steuermechanismen der Transaktion bereits über in der Anmeldung von Ginter et al. beschriebenen Verhandlungsmechanismen untereinander vereinbart wurden, und dass die verhandelten Regeln und Steuermechanismen zusammen mit der History der Verhandlung dieser Regeln und Steuermechanismen bei der obersten Transaktionsbehörde für die Immobilientransaktion gespeichert wurden. Die am höchsten stehende Transaktionsbehörde kann eine oberste Transaktionsbehörde **700** sein oder kann untereinander zwischen verteilten Transaktionsbehörden vereinbart worden sein. In diesem Beispiel nehmen wir ersteres an. Kurzgesagt haben alle Parteien den Regeln und Steuermechanismen, die die Transaktion regeln, zugestimmt. Der Verhandlungsprozess kann vereinfacht worden sein, da die Transaktionsbehörde **700** eine verteilte Template-Anwendung für internationale Immobilienverkäufe verteilt haben kann, wobei das Template dabei auf der in der Vergangenheit gesammelten Erfahrung der Transaktionsbehörde **700** basiert oder sie von der Transaktionsbehörde **700** insbesondere für diese Transaktion als einen Mehrwertdienst für ihre wichtigen Kunden erstellt wurde.

[0584] Jede der Parteien der Transaktion ist, gemäß den VDE-Regelsätzen, welche die atomare Transaktion definieren, verantwortlich dafür, nachzuprüfen, dass bestimmte Teile der Transaktion vor dem Abschluss der Gesamttransaktion abgeschlossen wurden. In einigen Fällen sind mehrere Parteien gemeinsam verantwortlich für das Abschließen von Teilen der Gesamttransaktion. Zum Beispiel müssen der Käufer und der Verkäufer einen Verkaufspreis vereinbart haben. In diesem Beispiel steuern sie ihre Geschäftsbedingungen bei, einschließlich, zum Beispiel, ihre Preise und andere Variablen, und sie verwenden die VDE-Verhandlungsmechanismen, um eine Vereinbarung zu treffen, die einen fairen Interes-

senausgleich darstellt. Wenn die elektronische Verhandlung nicht erfolgreich ist, dann müssen die Parteien direkt verhandeln, oder sichere VDE-Container mit Audit-Aufzeichnungen, die das Scheitern der Verhandlungen anzeigen, werden an die Transaktionsbehörde gesendet, die wiederum, jede der anderen Parteien, die autorisiert sind, an der Gesamttransaktion teilzunehmen, benachrichtigt.

[0585] Wenn die kaufende und die verkaufenden Parteien zustimmen, dann wird in diesem einen Beispiel eine Benachrichtigung von der geschützten VDE-Verarbeitungsumgebung an eine verteilte Transaktionsbehörde gesendet, die wiederum sämtliche andere Parteien einschließlich anderer teilnehmender Transaktionsbehörden benachrichtigt, wobei diese die Verhandlung abschließt (oder Anweisungen zum Abschluss der Verhandlungen erhält, die digital unter Benutzung von VDE-Techniken von beiden Parteien signiert wurden) und mitteilt, dass eine Vereinbarung bezüglich des Preises erzielt wurde. Basierend auf VDE-Regeln für Subtransaktionen kann die VDE eine Partei oder Parteien sicher darüber benachrichtigen, dass bestimmte weitere Subtransaktionen nun abgeschlossen werden sollen. In diesem Beispiel kann nun das Unternehmen für die Überprüfung von Grundstücksrechtstiteln (title search company) seine Aufgabe durchführen; ein Versicherungsunternehmen kann nun Verhandlungen mit dem Käufer bezüglich der Deckung beginnen und dabei die VDE-Verhandlungsmechanismen verwenden. Ein Anwalt in dem Beraterstab des Käufers kann Verhandlungen mit seinem Kollegen in dem Unternehmen des Verkäufers beginnen, beide internen Anwälte können während des Erstellens und Verhandelns der verschiedenen Dokumente, deren Ausführung Teile der Gesamttransaktion abschließt, mit ihrem externen Berater über die VDE und sichere VDE-Container interagieren.

[0586] In diesem Beispiel kann jede der Parteien eine oder mehr digitale Zertifikate besitzen, die von der zertifizierenden Behöre **500** ausgestellt wurden, um jede der Parteien dieser Transaktion und ihrer Subtransaktionen zu authentifizieren. Das Finanz-Clearinghaus **200** stellt einen Zahlungsvektor für verschiedene Mehrwertdienste bereit, in einem Beispiel für die, welche von der Transaktionsbehörde **700** bereitgestellt wurden. Das Usage-Clearinghaus **300** erfasst Audit-Aufzeichnungen, die von Zeit zu Zeit in sicheren VDE-Containern von jeder teilnehmenden geschützten VDE-Verarbeitungsumgebung gesendet wurden und stellt einen unabhängigen Audit dieser Transaktion durch eine dritte Partei bereit. Der sichere Verzeichnisdienst **600** unterstützt die Teilnehmer darin, die elektronischen Adressen der anderen zu lokalisieren und sichert gleichzeitig Vertrauenswürdigkeit und Geheimhaltung.

[0587] Wenn jede Subtransaktion abgeschlossen ist, dann benachrichtigt eine verteilte Transaktionsbehörde innerhalb der Organisation in welcher die Subtransaktion durchgeführt wurde, die oberste Behörde für diese Transaktion **700** darüber, dass diese Teilaufgabe abgeschlossen wurde. Gemäß den vorher vereinbarten VDE-Regelsätzen können einige oder alle Personen, die an der Transaktion beteiligt sind, auch über Audit-Aufzeichnungen und/oder Nachrichten, die von mindestens einer beteiligten geschützten VDE-Verarbeitungsumgebung sicher gesendet und von dieser authentifiziert wurden, benachrichtigt werden, einschließlich, zum Beispiel, PPEs an Knoten für Einzelpersonen, Distributed Commerce Utility Systemen, einer verteilten Transaktionsbehörde und/oder der obersten Behörde für diese Transaktion.

[0588] Wenn sämtliche Teilelemente der Gesamttransaktion abgeschlossen wurden, benachrichtigt eine Transaktionsbehörde, in diesem Beispiel die oberste Transaktionsbehörde für diesen Immobilienverkauf, jeden Teilnehmer und sämtliche beteiligte Transaktionsbehörden darüber, dass die Vorbedingungen erfüllt wurden und führt die Gesamttransaktion durch. Optional kann die Transaktionsbehörde dem Verkäufer und dem Käufer eine letzte Gelegenheit geben, den Abschluss durchzuführen oder die Transaktion noch zu verzögern. Dieses Beispiel zeigt, dass Commerce Utility Systeme **90**, einschließlich der Transaktionsbehörde **700** verteilt sein können, um zwischen geschützten VDE-Verarbeitungsumgebungen zu vermitteln, die eines oder mehr Commerce Utility Systeme **90** unterstützen.

Beispiel – Digitales Broadcasting Netzwerk

[0589] Das Amortisieren von Infrastruktur und anderen Ressourcen für viele Benutzer, das Aufbauen einer kritischen Masse in einem schnelleren Tempo als die Wettbewerber, das Unterstützen einer perfekt angepassten Spezialisierung und das Liefern der attraktivsten Produkte und Dienste an den Kunden, das Maximieren der Einflusskraft bei Verhandlungen für den Einkauf, und das Aufbauen der wettbewerbsfähigsten Infrastruktur, um als die beste Ressource aus einer Hand für ein bestimmtes Geschäftsfeld zu dienen – dies alles sind die zentralen Konzepte beim Aufbau einer modernen, erfolgreichen Geschäfts. VDE und Distributed Commerce Utility stellen eine Grundlage für das Aufbauen von in höchstem Maße wettbewerbsfähigen und erfolgreichen Cyberspace-Geschäften auf, welche diese Eigenschaften besitzen. Bei vielen derartigen Geschäftsformen werden Eigenschaften des Internet und des World Wide Web widergespiegelt. Wie VDE und Distributed Commerce Utility werden sie eine verteilte Gemeinschaft umfassen, die einen maximalen Vorteil durch das Unterstützen von elektronischen Handelspartnerschaften erzielt. Sie werden verschiedene Ebenen von Dienstleistungen und komplementären Produkten

und Diensten bereitstellen und werden einen großen Vorteil daraus haben, dass sie ihre Aktivitäten zu ihrem gegenseitigen Nutzen koordinieren.

[0590] Das Digitale Broadcasting Netzwerk ("DBN", Digital Broadcasting Network) wird solch ein derartiges innovatives, kommerzielles Unternehmen sein. Da es aus vielen verschiedenen, auf dem World Wide Web („WEB") basierenden Seiten und Diensten besteht, werden DBN-Teilnehmer größeren Einfluss und größere Betriebseffizienz durch das Teilen von Ressourcen gewinnen, sie werden dabei die maximale Kaufkraft erfahren und Marketing- und Kundendaten erzeugen und einen wirtschaftlichen Überbau unterstützen, der ihre vielen, oft komplementären Aktivitäten bündelt. In hohem Maße den konsistenten Regeln ähnlich, die sowohl das World Wide Weg als auch die Ausführungen von VDE und Distributed Commerce Utility ermöglichen und dessen Grundlage bilden, und auf Grundlage der Eigenschaften dieser beiden Architekturen, verwendet das digitale Broadcasting Netzwerk deren Erfindungen, um eine hocheffiziente, in hohem Maße automatisierte und verteilte Gemeinschaft, welche die Geschäftseffizienz maximiert, zu unterstützen. In ähnlicher Weise würden andere Beispiele weitere Gruppierungen von Einheiten, die als Virtuelle Unternehmen (z. B. Aktiengesellschaften oder andere Organisationen) funktionieren. Die verteilte Ausführung der VDE und des Commerce Utility Systems sind insbesondere wichtig, weil sie eine effiziente Infrastruktur für diese modernen, potentiell breit angelegten Cyberspace-Geschäftsaktivitäten bereitstellen.

[0591] Das digitale Broadcasting Netzwerk kann als eine Zusammenstellung von WEB-Seiten und, zum Beispiel Anbietern von Diensten dienen, mit einem zentralen und vielleicht regionalen oder logischen (z. B. marktbasierten) Hauptsitz, oder es kann als eine gewinnorientierte Shareholder-Aktiengesellschaft in einem Geschäftsmodell, das an Fernsehsendeanstalten (z. B. NBC) erinnern, dienen, oder als ein kooperatives oder virtuelles Unternehmen, dass eine Mischung oder eine Kombination von Mischungen der obigen Eigenschaften aufweist, und verteilte Peer-to-Peer, hierarchische und zentralisierte Verwaltungsgeschäftsbeziehungen und Aktivitäten verwenden. In einem Beispiel kann sich eine Vielzahl von Unternehmen zusammenschließen, um die Vorteile von Größe und Koordinierung mit einzelnen Teilnehmern, die jeder eine gewisse Art von Spezialwissen mitbringen und wobei der aus Einheiten zusammengesetzte koordinierte Gesamtkörper sich in einer Vereinigung oder einem Unternehmen „höherer" Ebene zusammenschließt.

[0592] In einem Beispiel kann das Digitale Broadcasting Netzwerk ein einzelnes Unternehmen sein, das viele lizenzierte Franchiseunternehmen besitzt. Die lizenzierten Franchiseunternehmen können Webseiten umfassen, die geographisch und/oder logisch spezialisierten Marktbereichen vorbehalten sind und/oder welche anderen Webseiten in einem hierarchischen und/oder Peer-to-Peer-Kontext von Diensten des Distributed Commerce Utility, wie oben beschrieben, dienen. Im Auftrag seiner selbst und seiner Franchiseunternehmen kann dieses Unternehmen zum Beispiel folgendes tun:

- optimale Preise für Sendezeiten mit Werbetreibenden und deren Agenturen verhandeln,
- die niedrigsten Preise für von Dritten zur Verfügung gestellte Inhalte erhalten,
- Marktanalysen und Benutzerprofildaten weiter verkaufen,
- seine Einkünfte mit den Franchiseunternehmen teilen, die wiederum ihre Einkünfte mit dem DBN- und/oder anderen Franchiseunternehmen teilen können,
- den Franchiseunternehmen als Antwort auf Franchiseprofilen und/oder Franchisebenutzerprofilen Werbung zur Verfügung stellen,
- eine gewisse Anzahl von „Augen" (Sendezeit und/oder weitere Interaktionen) in Bezug auf Werbematerial garantieren,
- ein sicheres virtuelles Netzwerk bereitstellen, das Fähigkeiten von VDE und Distributed Commerce Utility anwendet, sodass die Gesamtorganisation sicher und in höchstem Maße effizient arbeiten kann, einschließlich der Verwendung von gemeinsamen Benutzeranwendungstools, Benutzeroberflächen und Verwaltungsoperationen,
- Werbung für das Netzwerk zum Nutzen des Netzwerks und der Franchiseunternehmen machen,
- Inhalte erwerben und/oder auf andere Weise an Franchiseunternehmen liefern als Antwort auf Bedürfnisse von Franchiseunternehmen wie es in deren Anforderungen und/oder Benutzungsprofilen angezeigt wird,
- die Benutzung von Inhalten erfassen und analysieren (einschließlich Werbung), von Cyberspaceeinkäufen und anderen Daten, wie es durch die Vereinbarung mit Franchiseunternehmen erlaubt ist.
- es Franchiseunternehmen ermöglichen, viele Netzwerkfunktionen auf lokaler Ebene auszuführen – das heißt, geographisch und/oder logisch lokale Inhalte (konsistent mit deren Zielmarkt) zu erwerben und verfügbar zu machen (und/oder andere Inhalte, die für ihre Benutzerbasis von besonderem Interesse sind),
- Vereinbarungen hinsichtlich Werbematerial verhandeln, die auf dem physikalischen und/oder logischen Zielmarkt der Franchiseunternehmen von kommerziellem Wert sind,
- wenigstens einen Bereich seines WEB-„Broadcasting"-Raums überwachen, das heißt, lokale Kontrolle über wenigstens einen Bereich des Inhalts ausüben – mit der Instanz mit dem Recht auf diese Kontrolle und, zum Beispiel, bestärkt durch

Regeln und Steuermechanismen, die unter der Kontrolle des DBN und/oder einem oder mehr Netzwerkteilnehmern liegen, und

• Durchführen anderer Verwaltungs-, Unterstützungs- und/oder Dienstfunktionen im Auftrag von und/oder für das Netzwerk.

[0593] In einem Beispiel kann das DBN viele der Sicherheits- und Verwaltungsfähigkeiten des VDE und viele der Dienstfunktionen, die von den vorliegenden Erfindungen bereitgestellt werden, anwenden, um die verteilten Beziehungen und Aktivitäten, die zentral für das Geschäftsmodell des DBN sind, zu verwalten und zu automatisieren. Zum Beispiel:

• Transaktionsbehörde **700** kann den globalen Verwaltungskontext für das Verwalten der Netzwerkgemeinschaft bereitstellen. Zum Beispiel kann zertifizierende Behörde **700** folgendes tun: Sie kann (durch die Verwendung von VDE-Regeln und Steuermechanismen in der bevorzugten Ausführungsform) das Richten von Inhalten an bestimmte Franchiseuternehmen durchführen. Sie kann auch die zu dem Berichten der Benutzungsinformation gehörende Verbarbeitungs- und Steuerketten durchführen. Die Transaktionsbehörde **700** kann seine elektronischen Regelsätze von den Vertragsbeziehungen zwischen dem DBN und seinen Franchiseunternehmen erhalten und/oder ableiten. Elektronische Verhandlungen können verwendet werden, um diese Vertragsbeziehungen zu erstellen. Die Transaktionsbehörde **700** kann auch Regeln erhalten, die bilaterale oder andere Netzwerkbeziehungen direkt zwischen Franchiseunternehmen und anderen Beteiligten widerspiegeln.

• Rechte und Berechtigungs-Clearinghaus **400** kann kommerzielle Rechte, die sich auf Inhalte beziehen, auf Netzwerk-Franchiseunternehmen ausweiten. Es fungiert als ein Repository von Rechten die sich auf Inhalte beziehen und wird von Netzwerkeinheiten an Kunden geliefert- einschließlich Rechten auf Inhalte, die Netzwerkeinheiten selbst gehören und die anderen Netzwerkeinheiten zugänglich gemacht wurden. Derartige Inhaltsrechte können zum Beispiel das Anzeigen, Verkaufen, Wiederverkaufen, Umrichten und Werben einschließen. Es kann auf Anfrage zusätzliche Rechte bereitstellen (z. B. Wiederverkaufsrechte oder besondere Umrichtrechte) und/oder automatisiertes Erstellen von Profilen, zum Beispiel je nach Benutzung.

• Usage Clearinghaus **300** kann Benutzungsdaten zur Unterstützung von Marktanalysen, dem Erstellen von Benutzungsprofilen und dem Werben sammeln. Es kann auch diese Information analysieren und Berichte daraus erstellen. Es kann diese Berichte intern an das DBN verteilen und Berichte verkaufen und/oder weitere Benutzungsinformation extern auf Grundlage von kommerziellen Möglichkeiten verteilen.

• Finanz-Clearinghaus **200** kann eine angemessene Ausführung der Entschädigung in dem Netzwerk gewährleisten. Es kann von Franchiseunternehmen Zahlungen für Inhalte an das DBN einziehen. Es kann Zahlung an Franchiseunternehmen verteilen, die sie als Ergebnis von Werbung und Wiederverkauf von Benutzungsinformation erhalten. Es kann Zahlungen von Franchiseunternehmen für die Unterstützungen der DBN-Infrastruktur und von Dienstleistungen, wie zum Beispiel Netzwerkwerbung, einziehen. Es verbindet sich mit der allgemein anwendbaren Finanz-Clearinghaus-Infrastruktur, um Daten in Bezug auf Zahlungen zu übertragen und zu erhalten.

• Der sichere Verzeichnisdienst **600** kann Verzeichnisdienste, die auf eindeutigen Kennungen und/oder einem oder mehr Klassenattributen basieren, unterhalten. Es kann global eine sehr große Anzahl von Franchiseunternehmen geben. Verzeichnisdienste **600** könnten auch Verzeichnisdaten über Kunden unterhalten, einschließlich eindeutiger Kennungs- und Profildaten. Sichere Verzeichnisdienste **600** können eine Verzeichnisinfrastruktur für Inhalte unterhalten, die das Netzwerk besitzt, verwaltet und/oder die ihm zugänglich sind.

• Eine zertifizierende Behörde **500** kann die Rollen aller Teilnehmer in dem Netzwerk zertifizieren. Sie könnte zum Beispiel ein Zertifikat für jedes Franchiseunternehmen ausstellen. Sie könnte auch Zertifikate ausstellen, die kommerzielle Beziehungen von Gruppierungen von Netzwerkeinheiten zertifizieren, um effiziente, sichere Beziehungen mit Dritten zu vereinfachen. Sie können auch Zertifikate an Kunden ausgeben, um bestimmte spezielle Kundenrechte hinsichtlich kommerzieller Aktivitäten von Kunden mit externen Parteien (zum Beispiel, Rabatte oder die Tatsache, dass man ein Mitglied der größeren „DBN"-Gemeinschaft ist) zertifizieren.

[0594] Teile von oder sämtliche spezielle Dienstleistungsfunktionen (z. B. wie oben beschrieben) können in höchstem Maße verteilt sein und können signifikant, primär oder sogar ausschließlich auf Netzwerk-Webservern von Franchiseunternehmen und Diensten laufen.

Patentansprüche

1. Ein Verfahren für das Zugreifen auf digitalen Inhalt unter Verwendung einer Vorrichtung für den elektronischen Handel und/oder für die Verwaltung von Rechten, wobei die Vorrichtung folgendes umfasst:

ein benutzerseitiges elektronisches Gerät (**100**) mit einer geschützten Verarbeitungsumgebung (**154**),

ein zweites elektronisches Gerät (**100'**), und

ein elektronisches Datenübertragungsnetzwerk (**150**), das dem benutzerseitigen Gerät (**100**) und

dem zweiten Gerät (**100'**) ermöglicht, digitale Signale auszutauschen,
wobei das Verfahren die folgenden Schritte umfasst:
Senden einer Anfrage bezüglich eines Zugriffs auf den digitalen Inhalt von dem benutzerseitigen Gerät (**100**) an das zweite Gerät (**100'**),
Empfangen von digitalem Inhalt aus dem zweiten Gerät (**100'**) an dem benutzerseitigen Gerät (**100**) sowie eines assoziierten Satzes von Regeln und Steuermechanismen (**188**),
Empfangen eines digitalen Zertifikats von einer zertifizierenden Behörde (**500**) an dem benutzerseitigen Gerät (**100**), das mindestens ein Attribut des Benutzers attestiert, wobei die Regeln und Steuermechanismen (**188**) eine Benutzung des empfangenen Inhalts, die vom Empfang eines geeigneten digitalen Zertifikats abhängig ist, definiert und der Satz von Regeln und Steuermechanismen (**188**) von der geschützten Verarbeitungsumgebung (**154**) umgesetzt wird.

2. Das Verfahren gemäß Anspruch 1, das ferner den Schritt des Messens der Benutzung des digitalen Inhalts an dem benutzerseitigen Gerät umfasst.

3. Das Verfahren gemäß Anspruch 1, das ferner den Schritt des Ausführens mindestens einer Mikro-Zahlungs-Aggregationsaufgabe an dem benutzerseitigen Gerät (**100**) umfasst.

Es folgen 100 Blatt Zeichnungen

Anhängende Zeichnungen

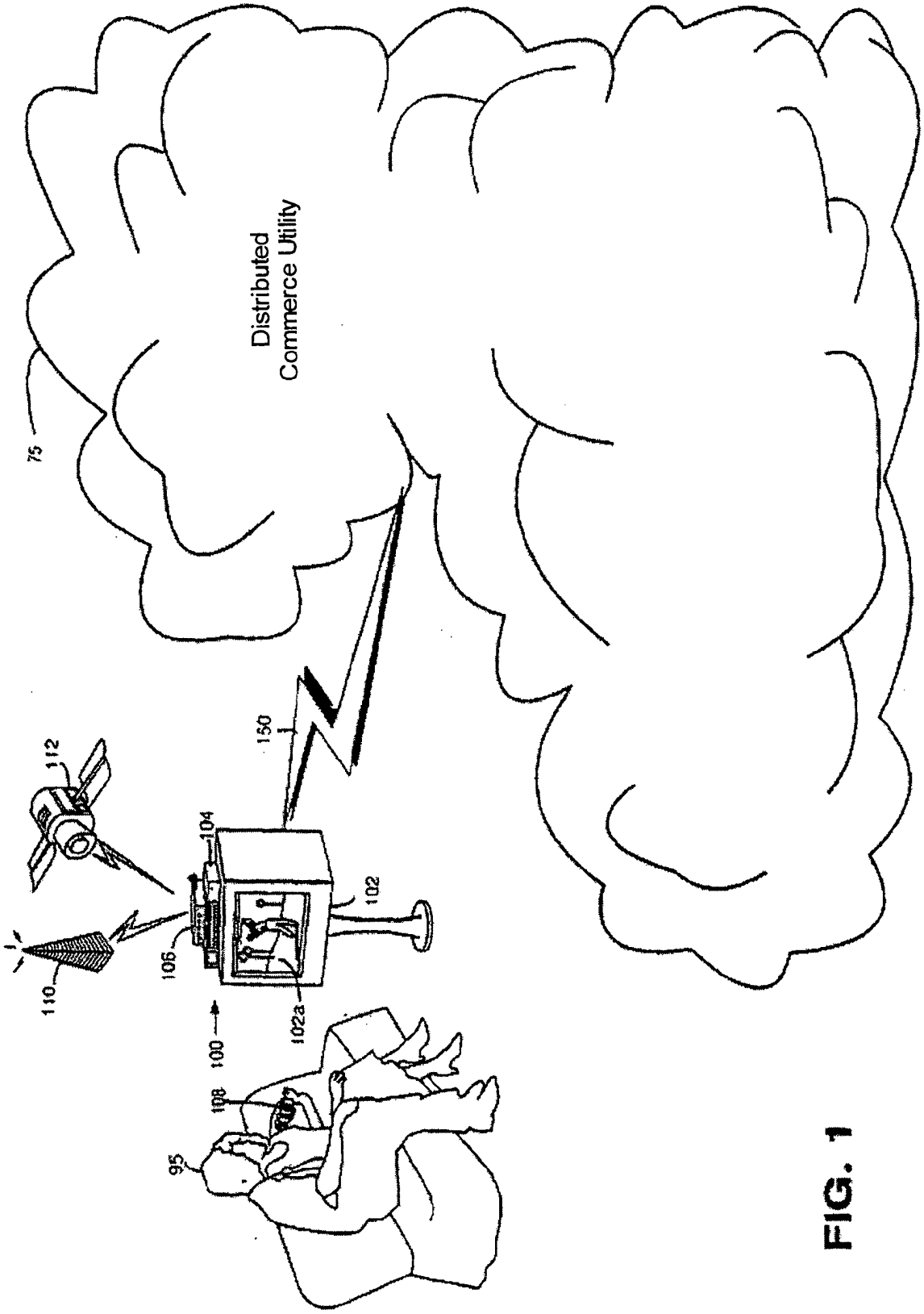
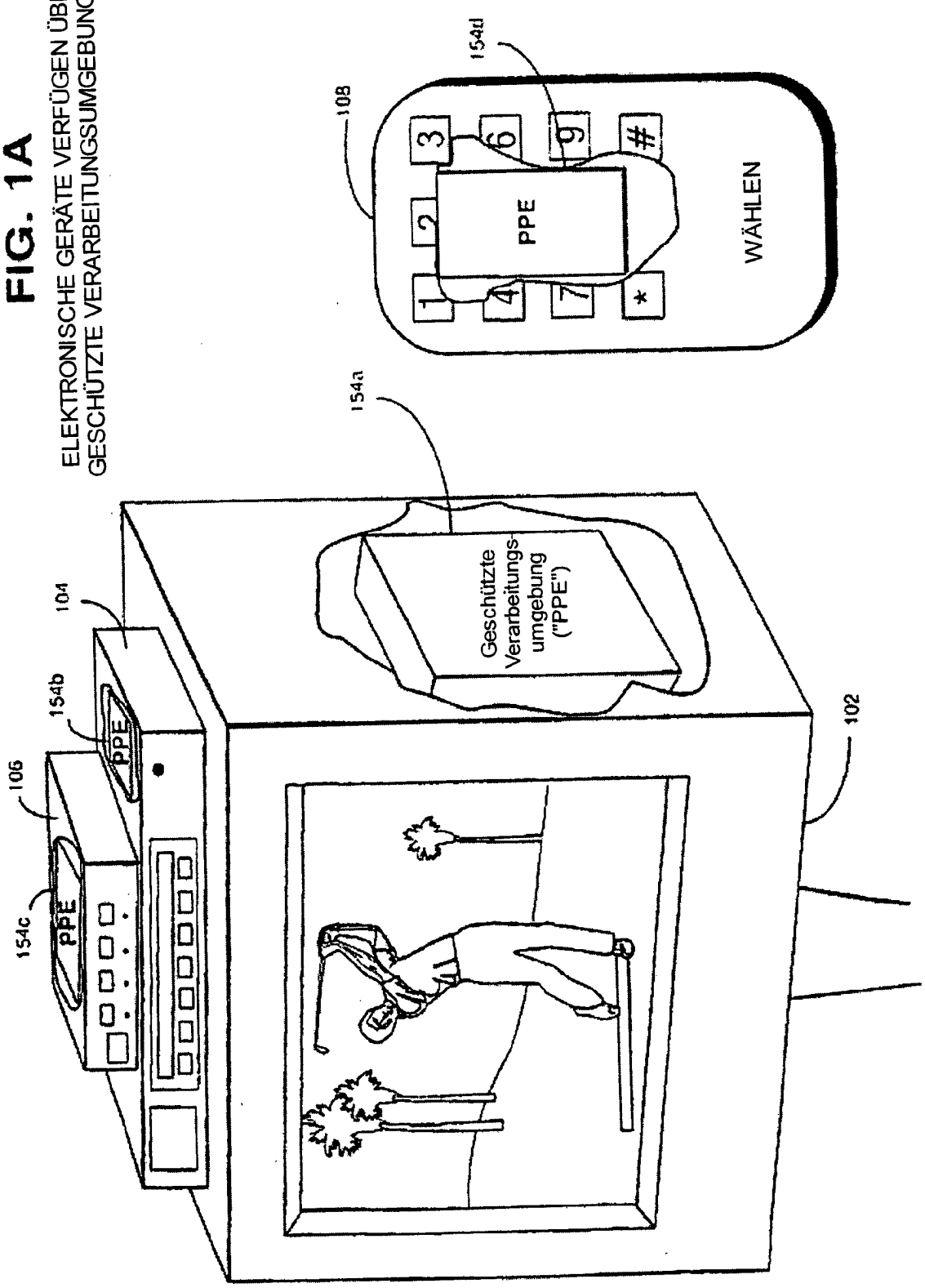


FIG. 1

FIG. 1A

ELEKTRONISCHE GERÄTE VERFÜGEN ÜBER GESCHÜTZTE VERARBEITUNGSUMGEBUNGEN



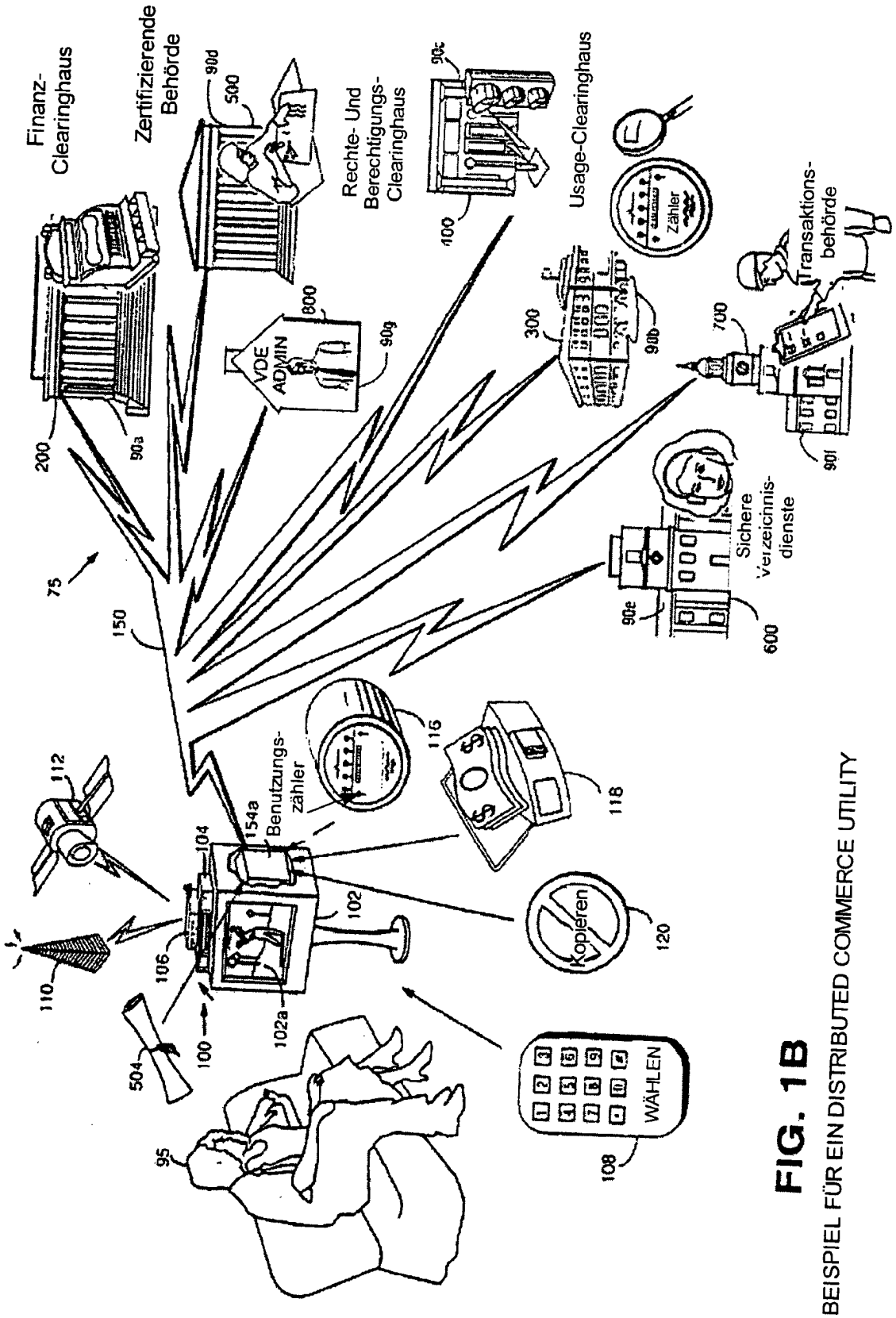


FIG. 1B

BEISPIEL FÜR EIN DISTRIBUTED COMMERCE UTILITY

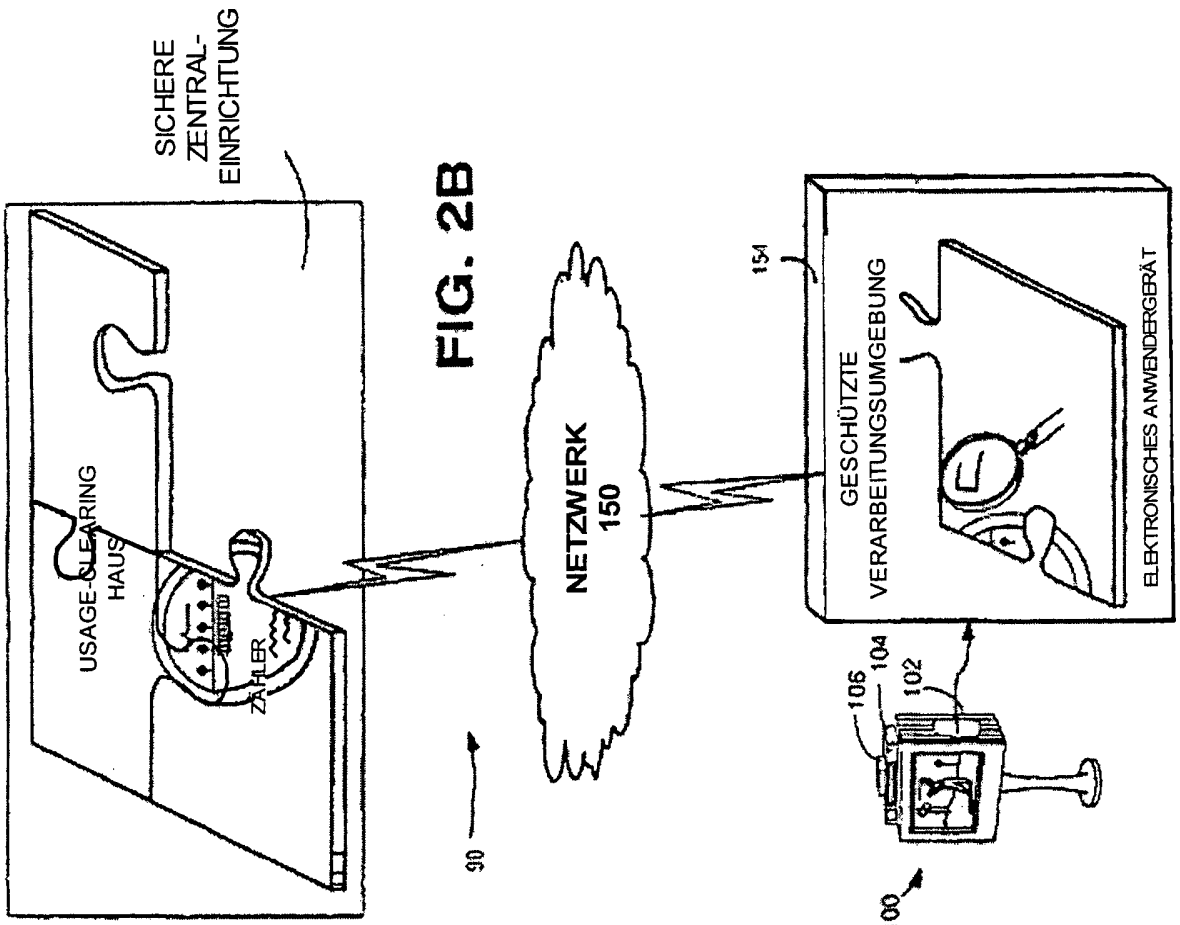

SICHERE ZENTRAL-EINRICHTUNG
USAGE-CLEARING HAUS
ZÄHLER
NETZWERK 150
GESCHÜTZTE VERARBEITUNGSUMGEBUNG
ELEKTRONISCHES ANWENDERGERÄT
154
106
104
102
100
90

FIG. 2B

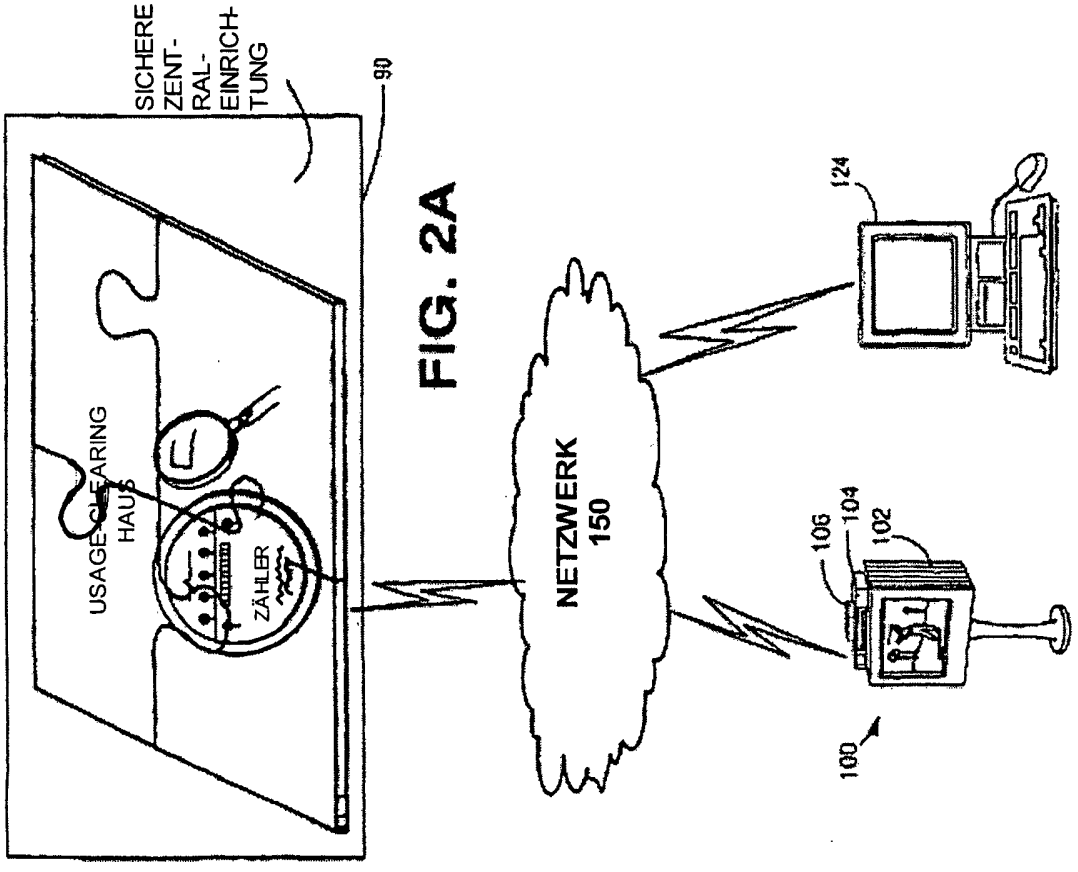

SICHERE ZENT-RAL-EINRICH-TUNG
90
USAGE-CLEARING HAUS
ZÄHLER
NETZWERK 150
124
106
104
102
100

FIG. 2A

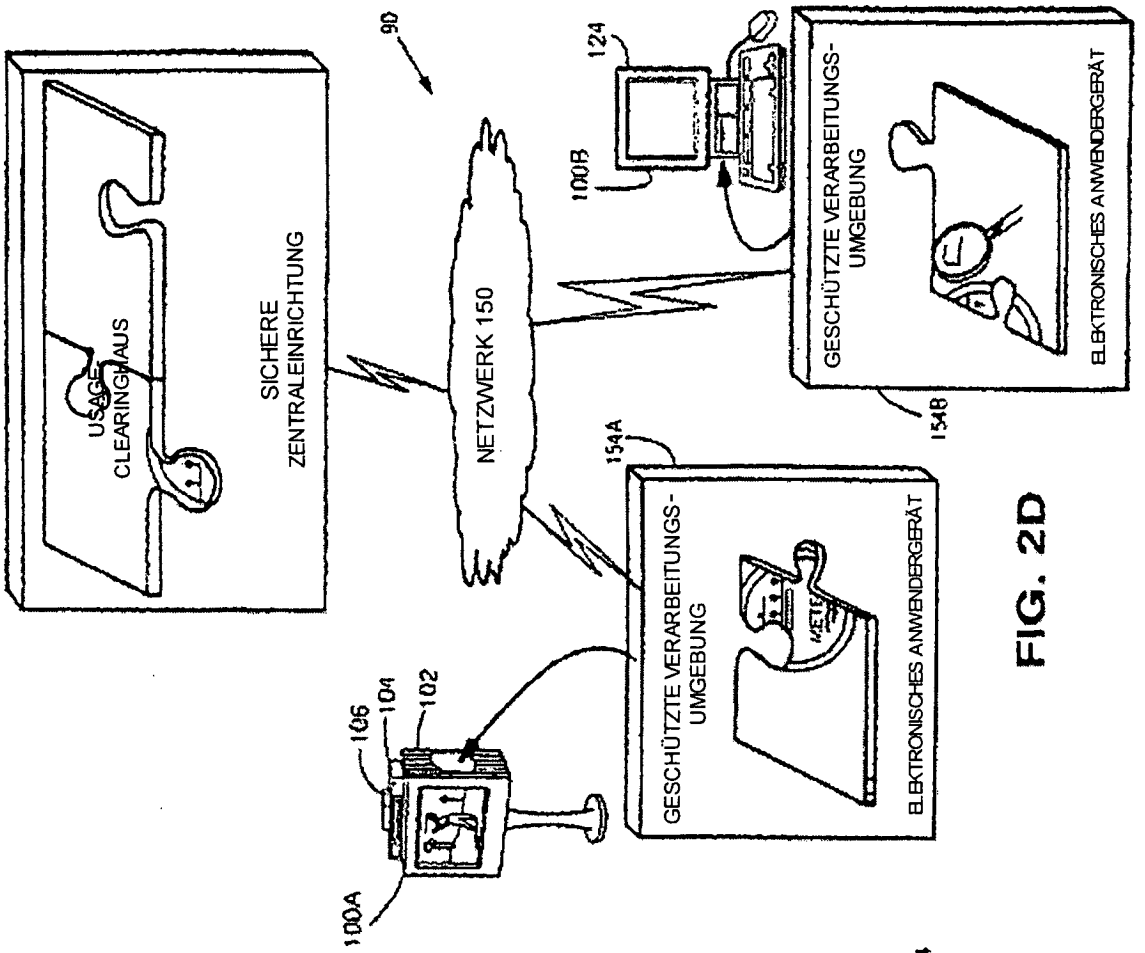

SICHERE ZENTRALEINRICHTUNG
USAGE CLEARINGHAUS
NETZWERK 150
90
124
100B
GESCHÜTZTE VERARBEITUNGS-UMGEBUNG
ELEKTRONISCHES ANWENDERGERÄT
154B
154A
GESCHÜTZTE VERARBEITUNGS-UMGEBUNG
ELEKTRONISCHES ANWENDERGERÄT
106
104
102
100A

FIG. 2D

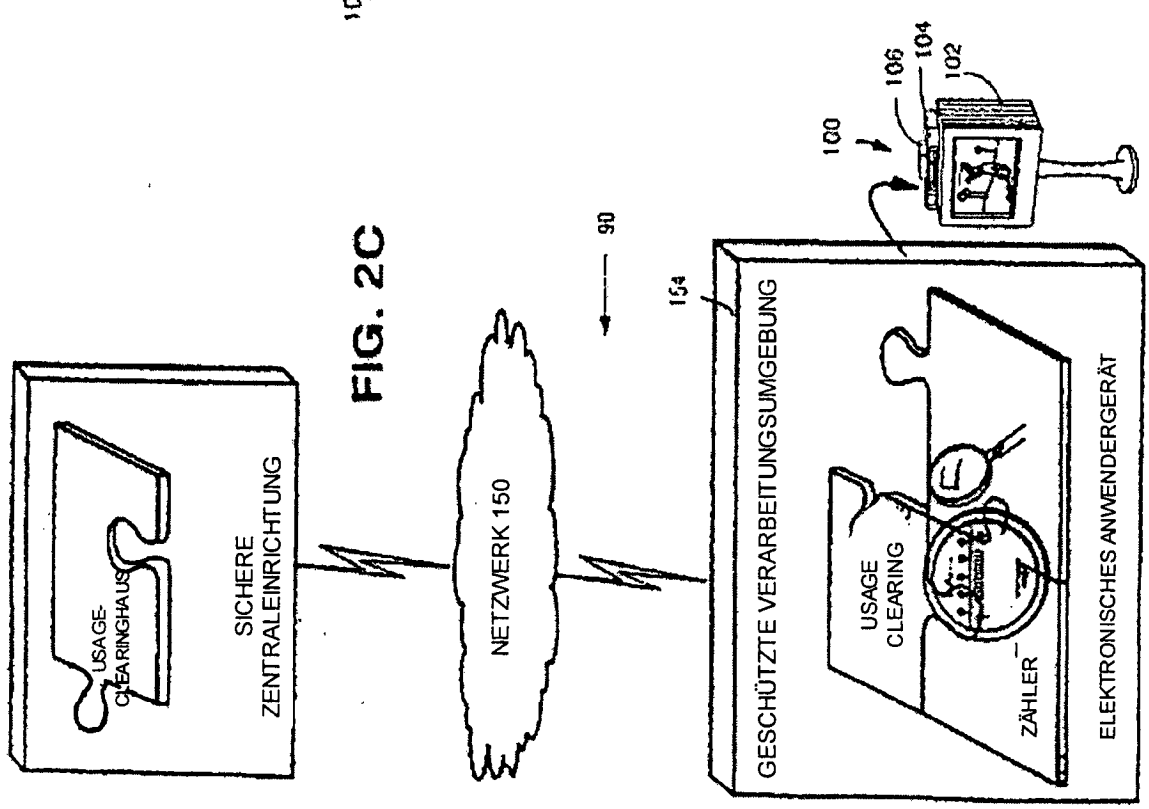

SICHERE ZENTRALEINRICHTUNG
USAGE-CLEARINGHAUS
NETZWERK 150
90
154
GESCHÜTZTE VERARBEITUNGSUMGEBUNG
USAGE CLEARING
ZÄHLER
ELEKTRONISCHES ANWENDERGERÄT
100
106
104
102

FIG. 2C

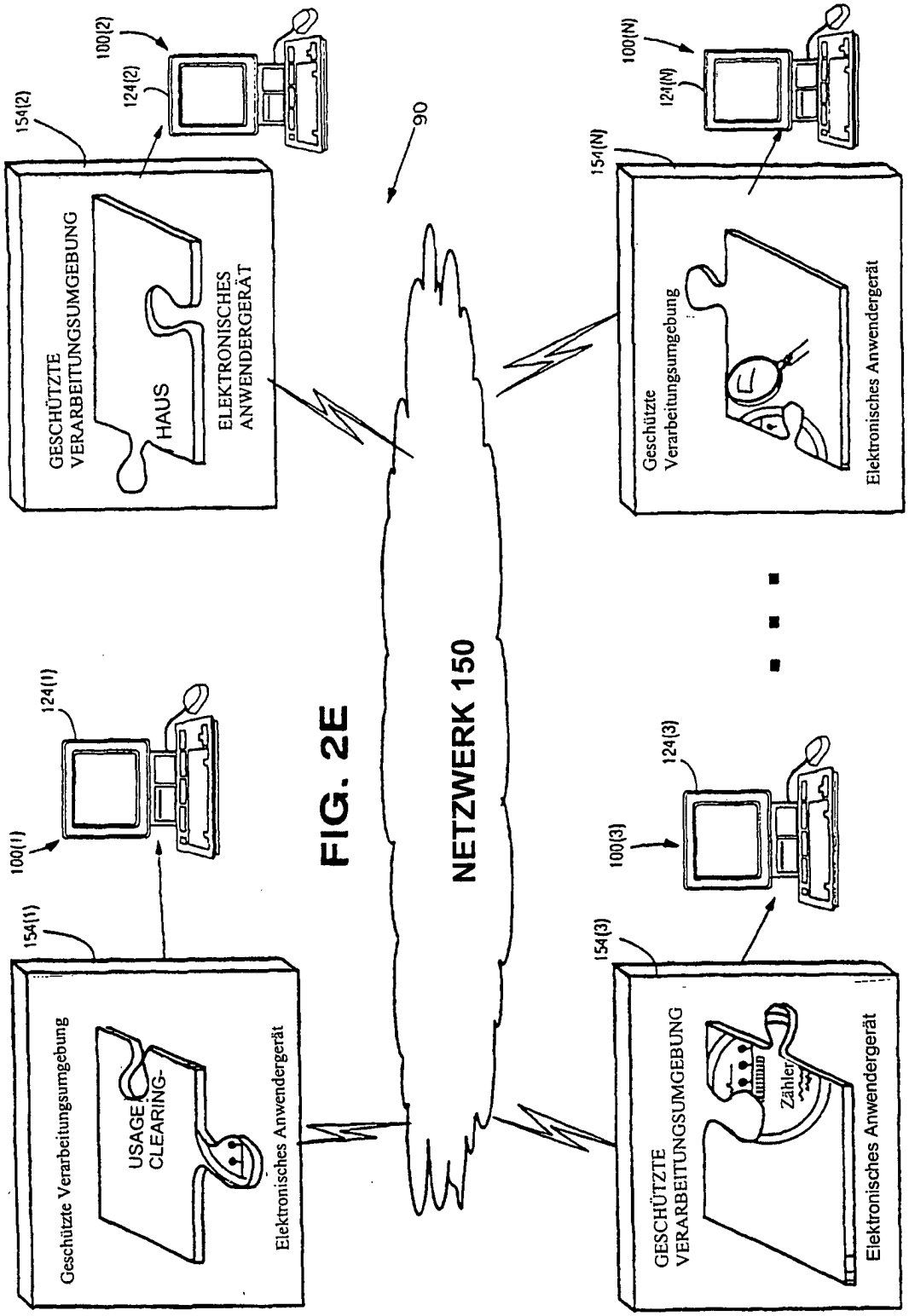

90
NETZWERK 150
100(2)
124(2)
154(2)
GESCHÜTZTE VERARBEITUNGSUMGEBUNG
HAUS
ELEKTRONISCHES ANWENDERGERÄT
100(N)
124(N)
154(N)
Geschützte Verarbeitungsumgebung
Elektronisches Anwendergerät
100(1)
124(1)
154(1)
Geschützte Verarbeitungsumgebung
USAGE CLEARING-
Elektronisches Anwendergerät
100(3)
124(3)
154(3)
GESCHÜTZTE VERARBEITUNGSUMGEBUNG
Zähler
Elektronisches Anwendergerät

FIG. 2E

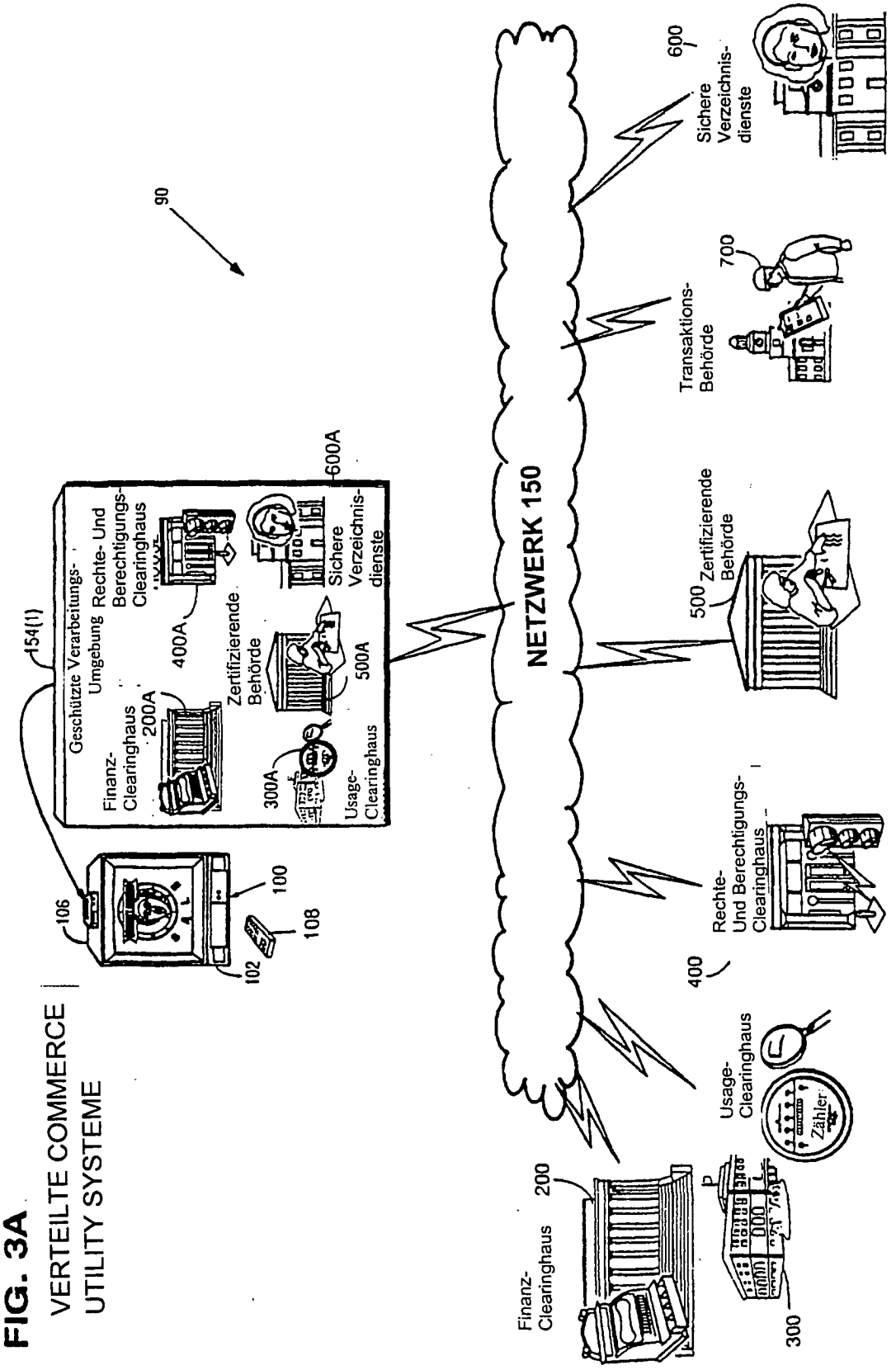


FIG. 3A
VERTEILTE COMMERCE
UTILITY SYSTEME

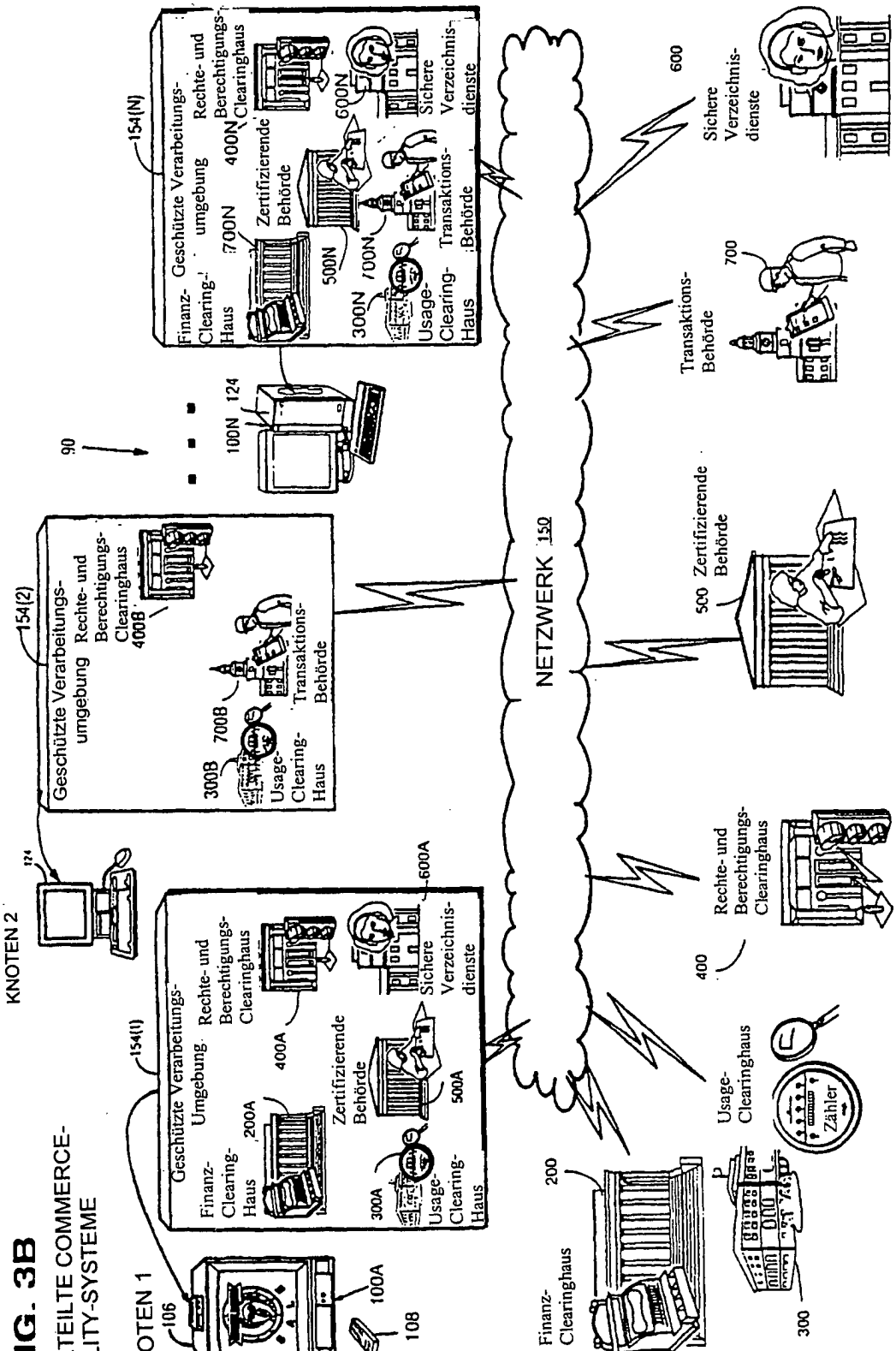


FIG. 3B

VERTEILTE COMMERCE-UTILITY-SYSTEME

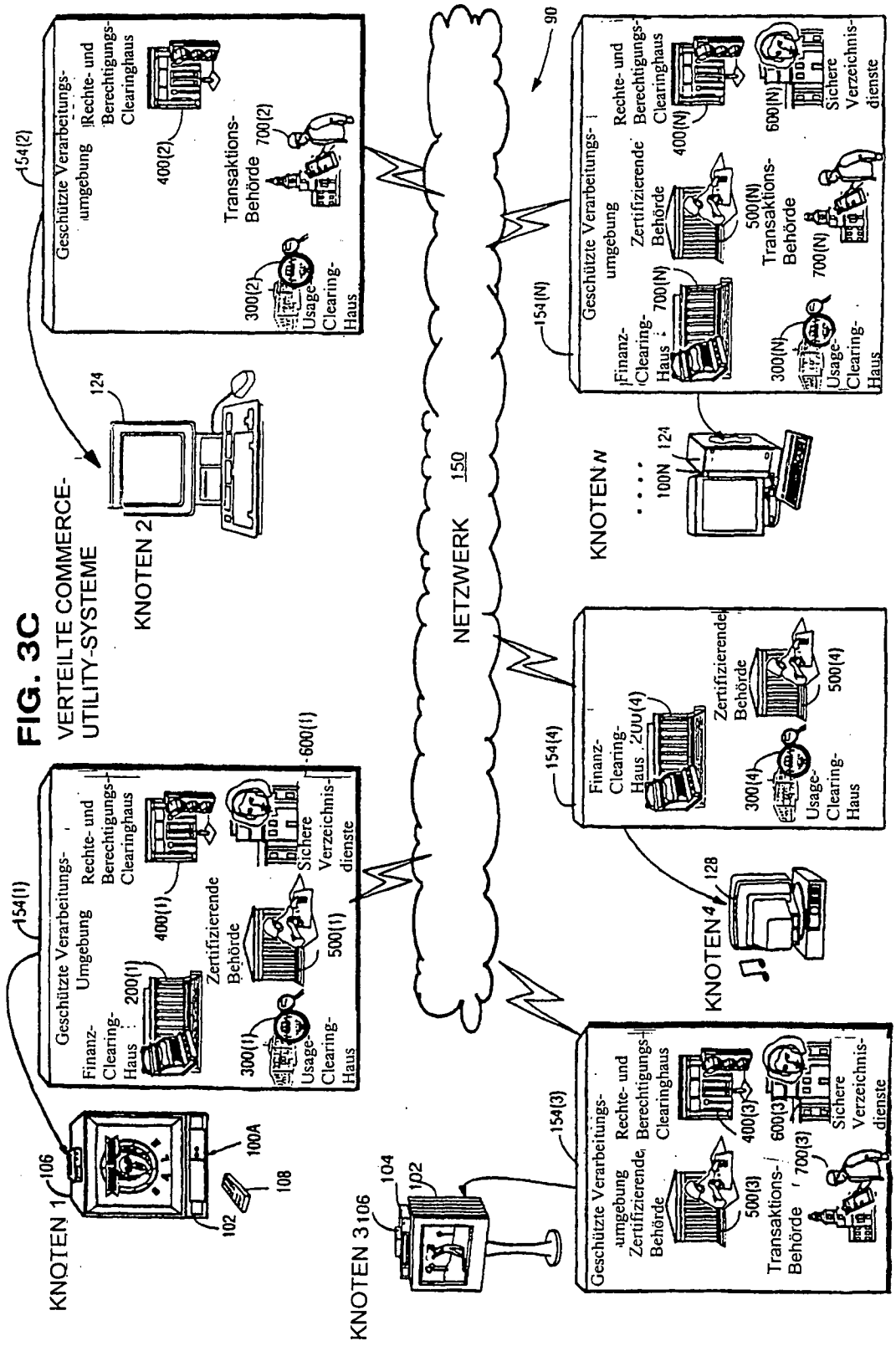


FIG. 3C
VERTEILTE COMMERCE-UTILITY-SYSTEME
KNOTEN 1
KNOTEN 2
KNOTEN 3
KNOTEN 4
KNOTEN N
NETZWERK 150
90
Geschützte Verarbeitungs-umgebung
Finanz-Clearing-Haus
Rechte- und Berechtigungs-Clearinghaus
Zertifizierende Behörde
Transaktions-Behörde
Usage-Clearing-Haus
Sichere Verzeichnis-dienste
154(1)
154(2)
154(3)
154(4)
154(N)
100A
100N
102
104
106
108
124
128
200(1)
300(1)
300(2)
300(3)
300(4)
300(N)
400(1)
400(2)
400(3)
400(N)
500(1)
500(3)
500(4)
500(N)
600(1)
600(3)
600(N)
700(2)
700(3)
700(N)

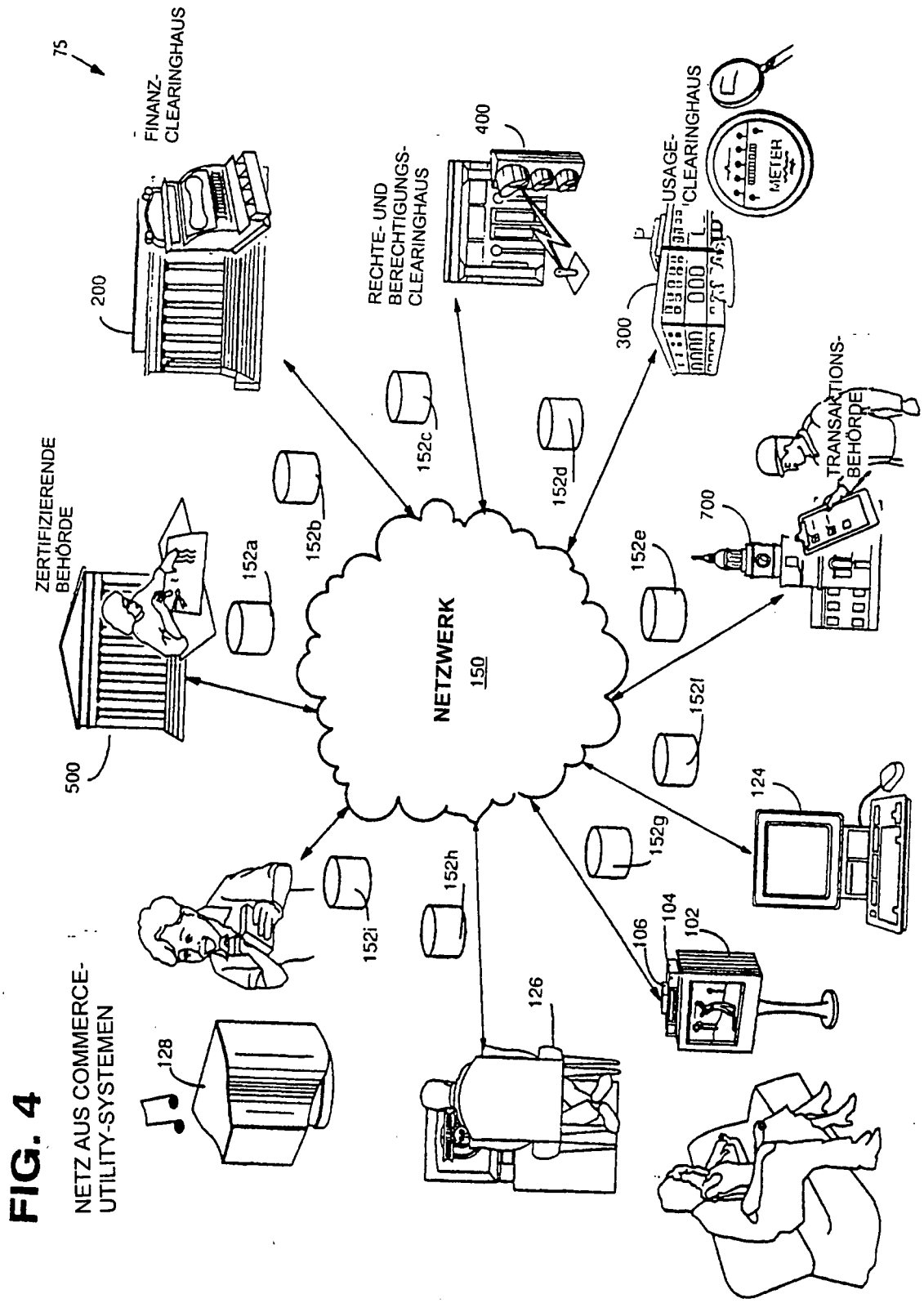


FIG. 4

NETZ AUS COMMERCE-UTILITY-SYSTEMEN

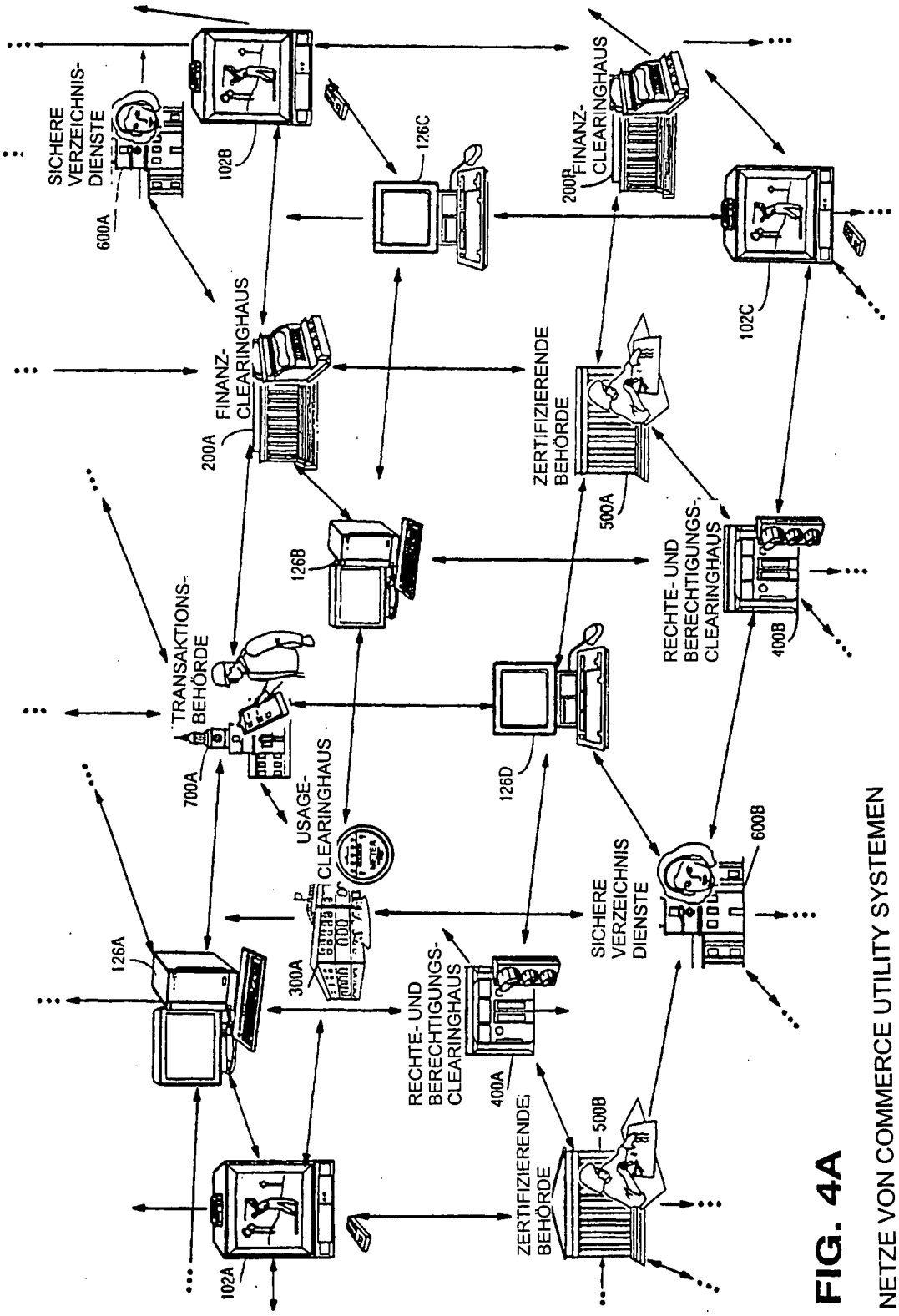


FIG. 4A

NETZE VON COMMERCE UTILITY SYSTEMEN

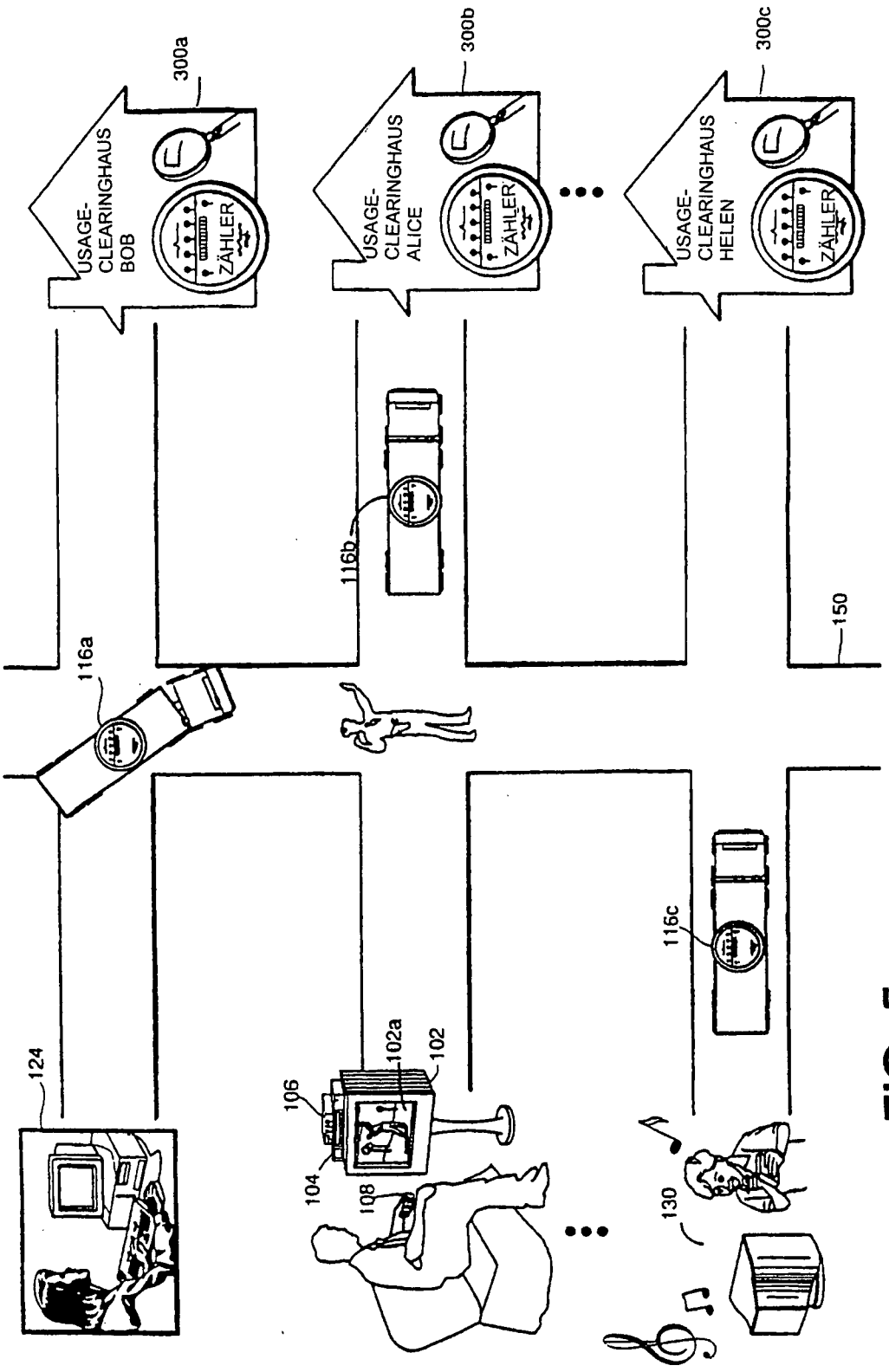


FIG. 5

RECHTEINHABER KÖNNEN ZWISCHEN COMMERCE-UTILITY-SYSTEMEN WÄHLEN

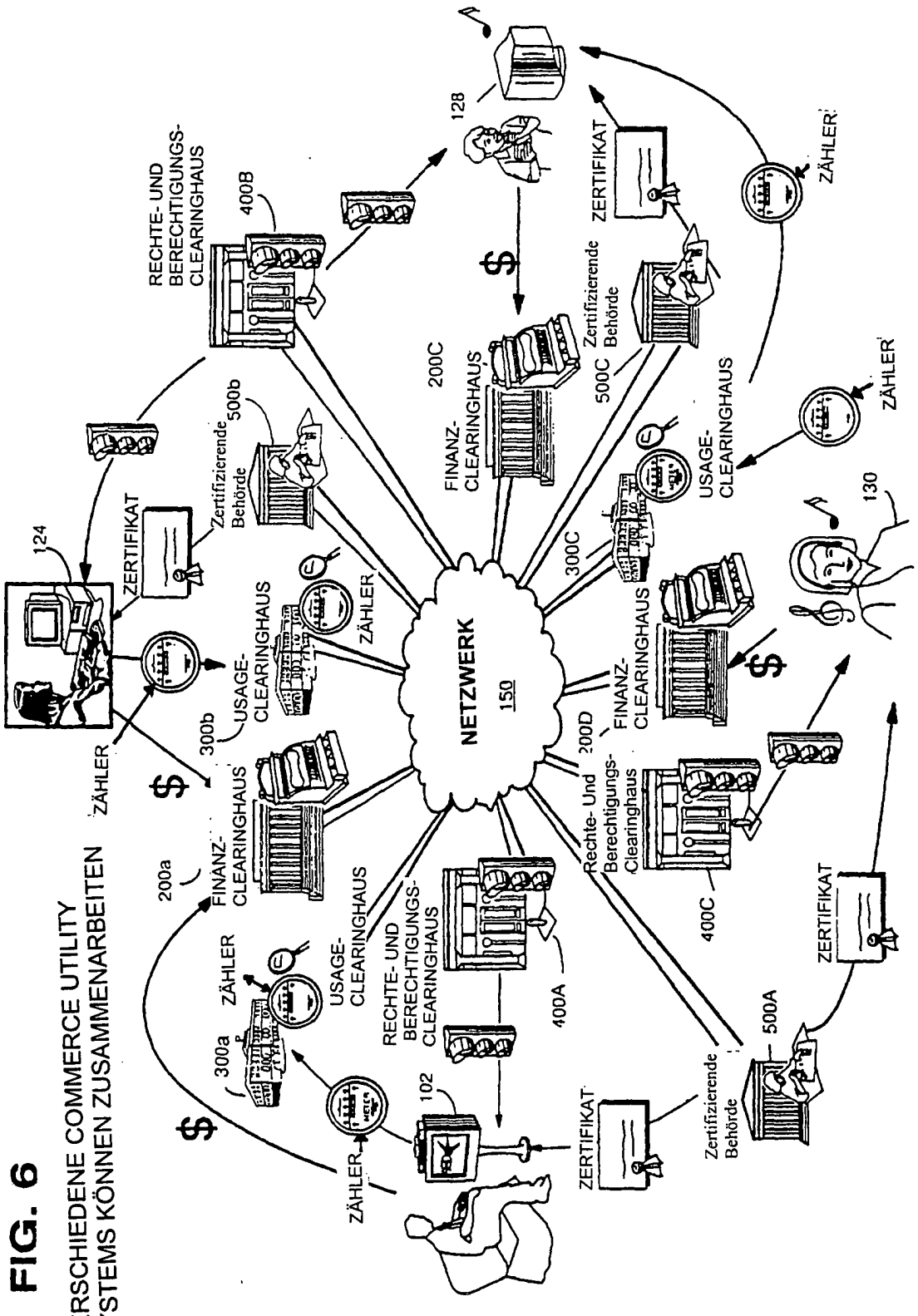


FIG. 6

VERSCHIEDENE COMMERCE UTILITY SYSTEMS KÖNNEN ZUSAMMENARBEITEN

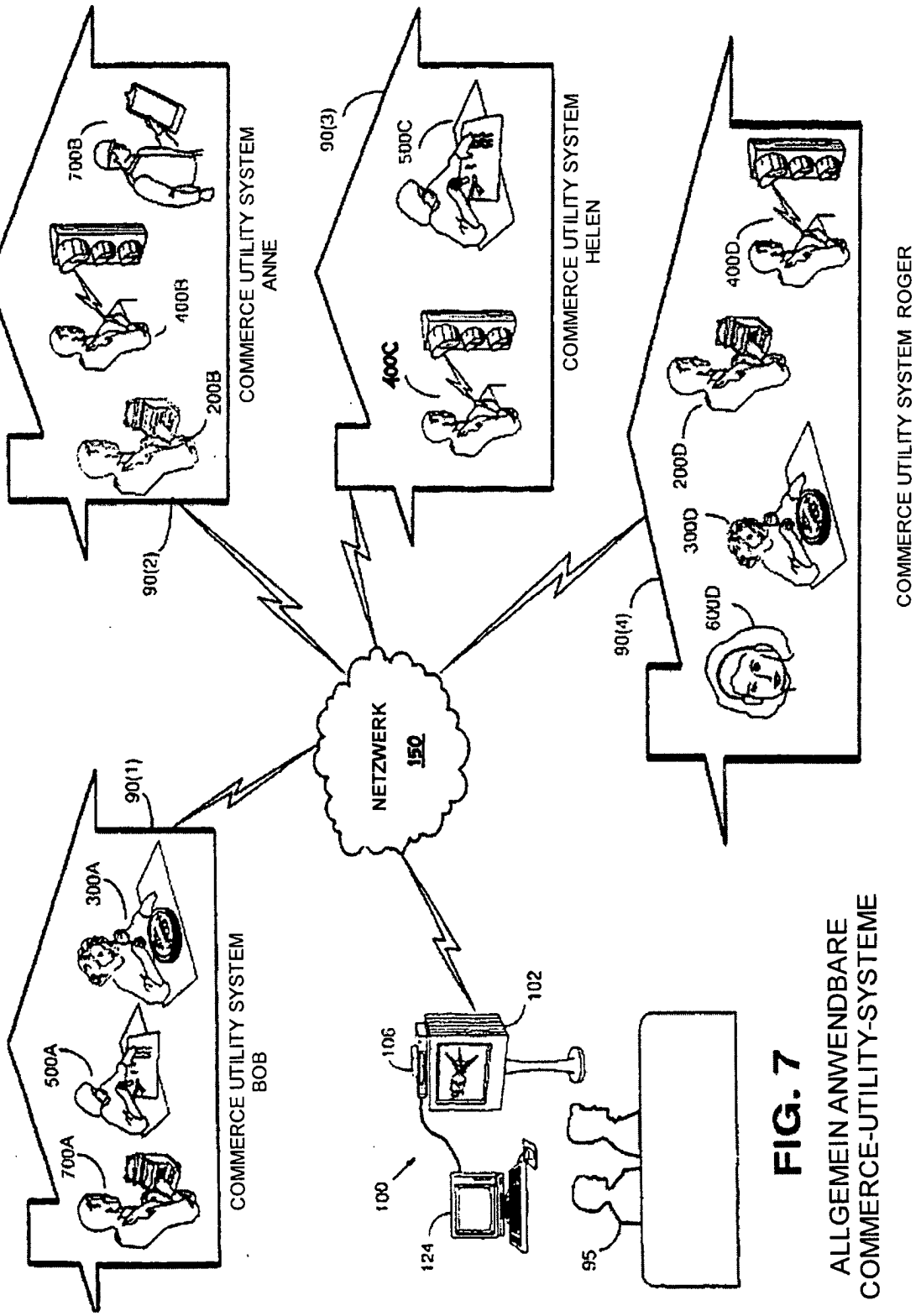


FIG. 7

ALLGEMEIN ANWENDBARE
COMMERCE-UTILITY-SYSTEME

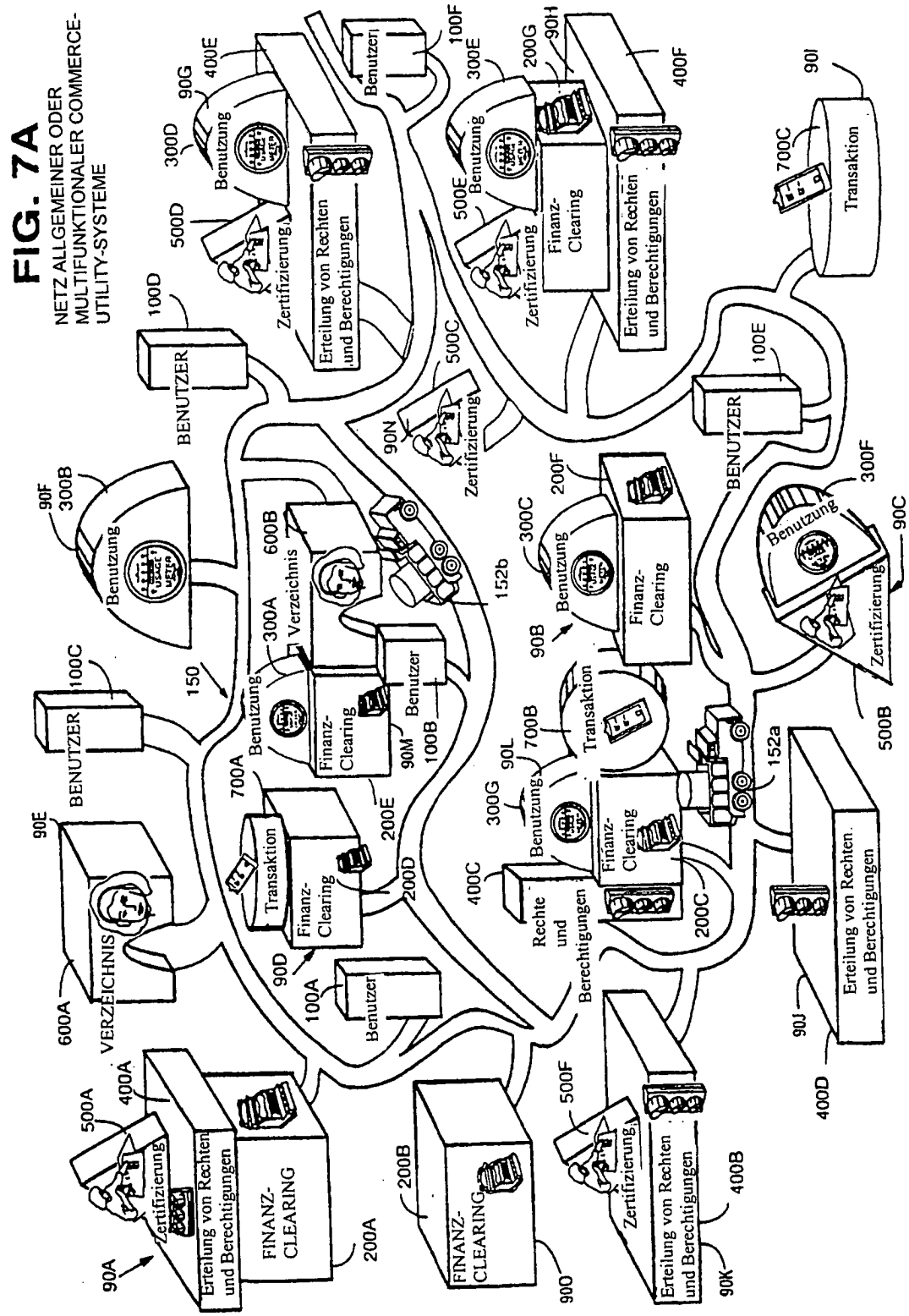

NETZ ALLGEMEINER ODER MULTIFUNKTIONALER COMMERCE-UTILITY-SYSTEME
BENUTZER
VERZEICHNIS
FINANZ-CLEARING
Zertifizierung
Erteilung von Rechten und Berechtigungen
Benutzung
Verzeichnis
Finanz-Clearing
Transaktion
Rechte und Berechtigungen
Benutzer
90A
90B
90C
90D
90E
90F
90G
90H
90I
90J
90K
90L
90M
90N
90O
100A
100B
100C
100D
100E
100F
150
152a
152b
200A
200B
200C
200D
200E
200F
200G
300A
300B
300C
300D
300E
300F
300G
400A
400B
400C
400D
400E
400F
500A
500B
500C
500D
500E
500F
600A
600B
700A
700B
700C

FIG. 7A

FIG. 8A

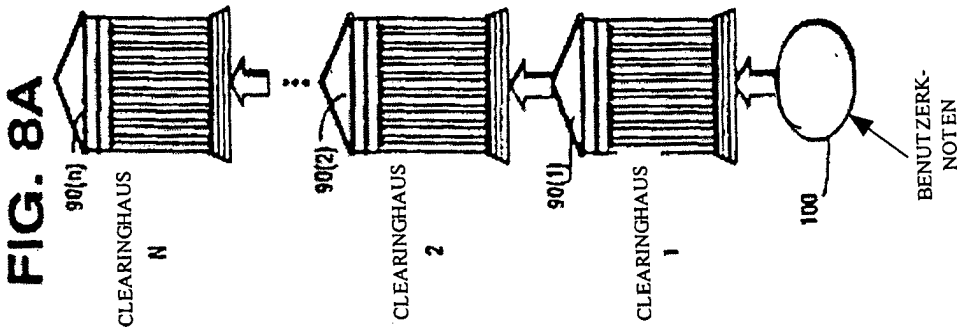


FIG. 8B

HIERARCHIE VON COMMERCE UTILITY SYSTEMS

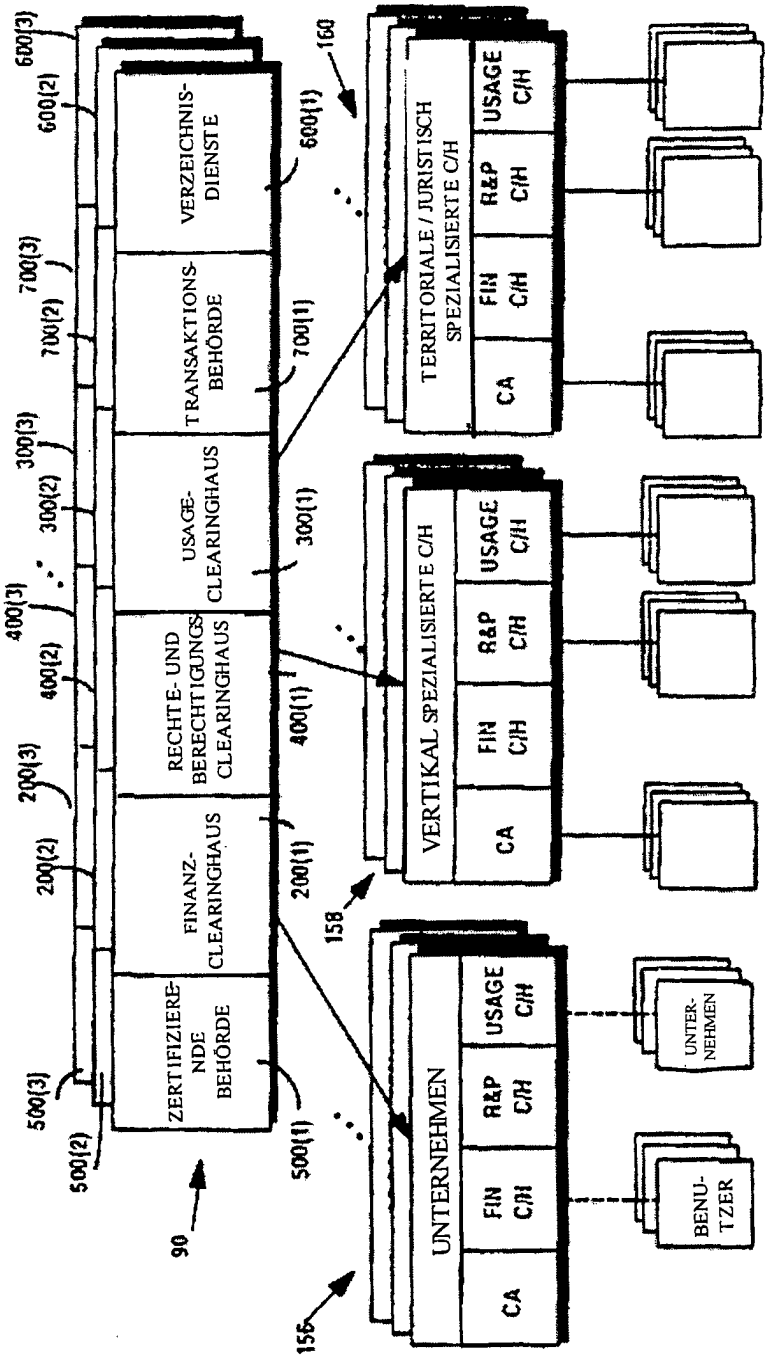
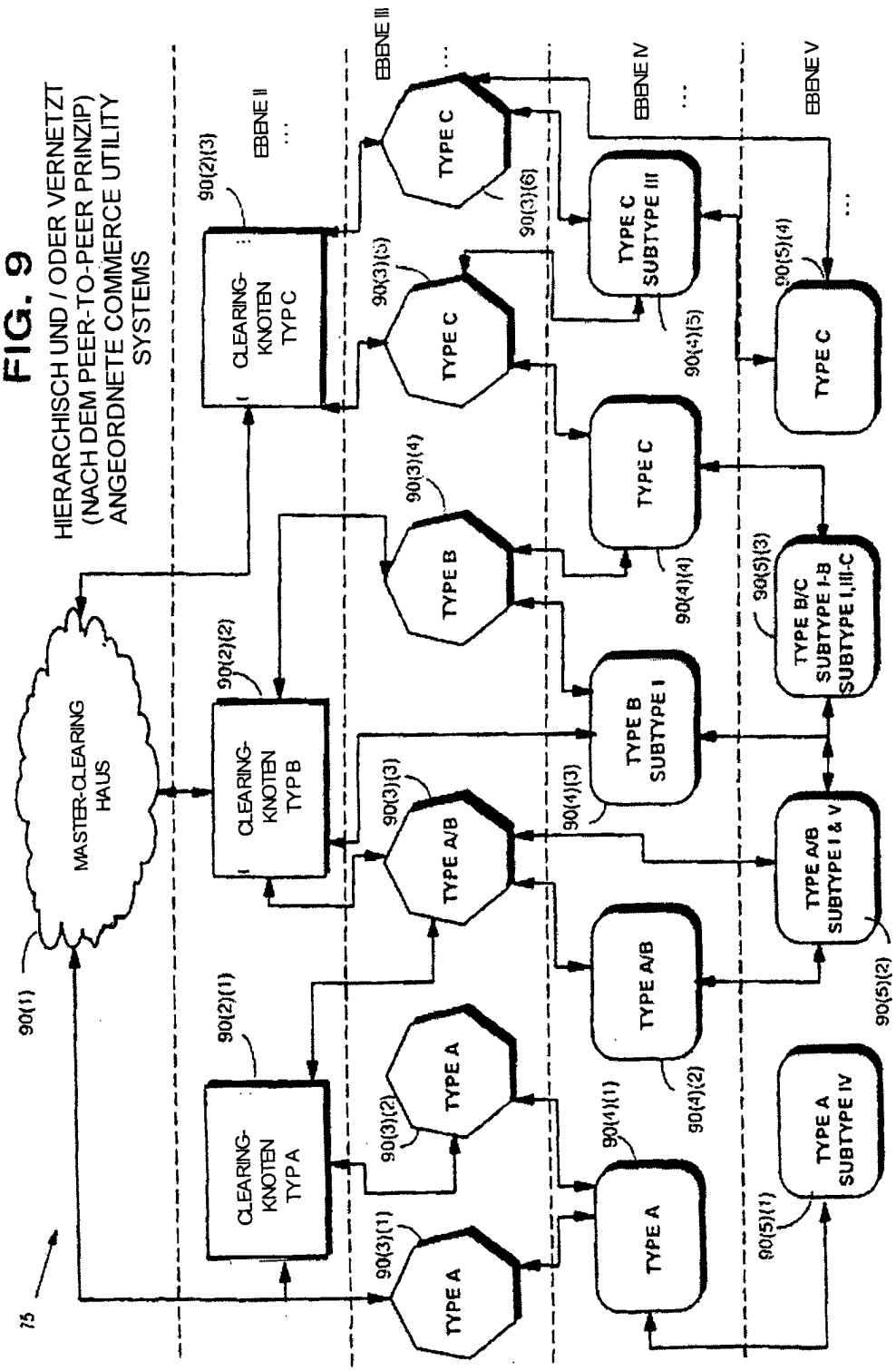


FIG. 9

HIERARCHISCH UND / ODER VERNETZT
(NACH DEM PEER-TO-PEER PRINZIP)
ANGEORDNETE COMMERCE UTILITY
SYSTEMS



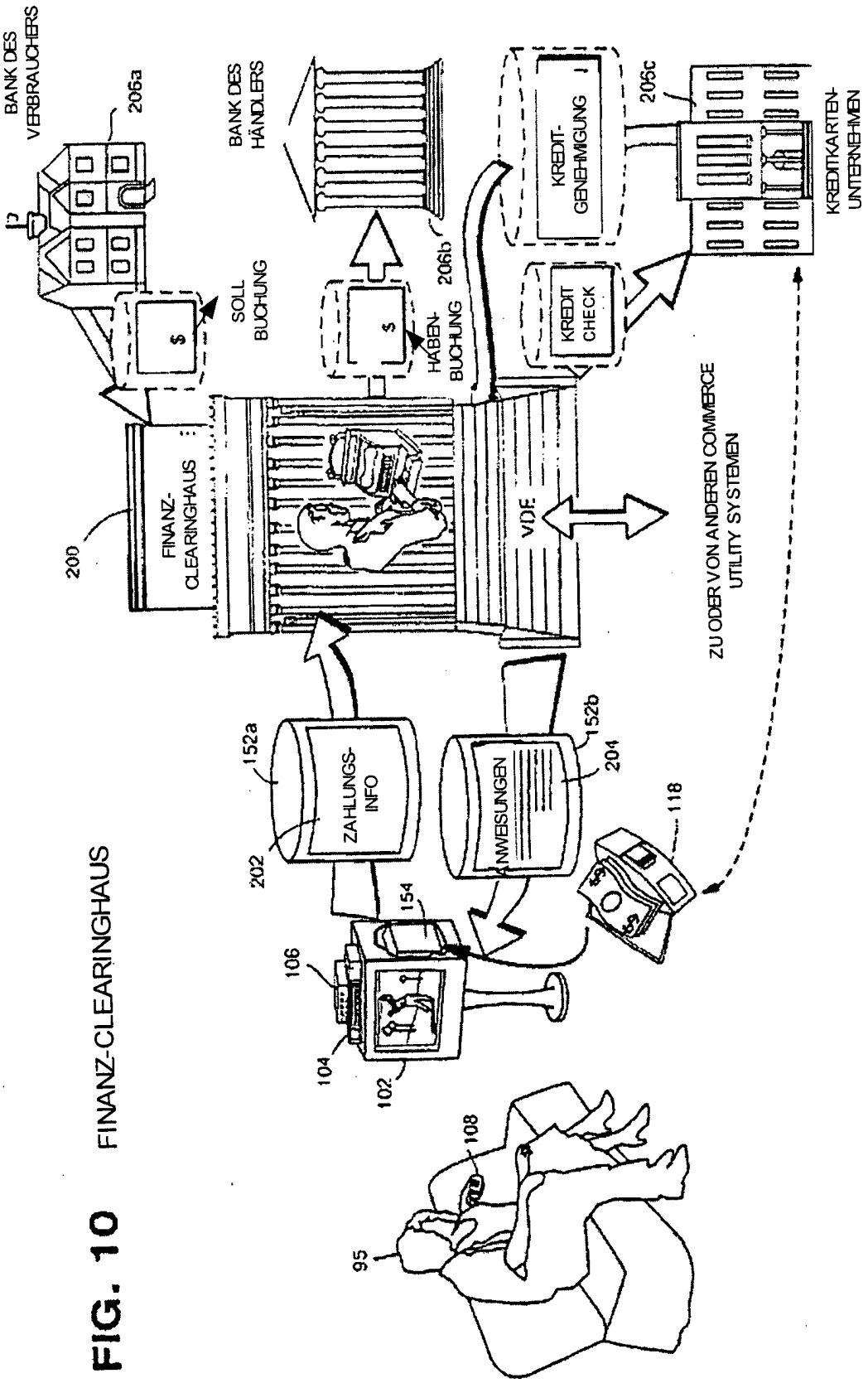


FIG. 10 FINANZ-CLEARINGHAUS

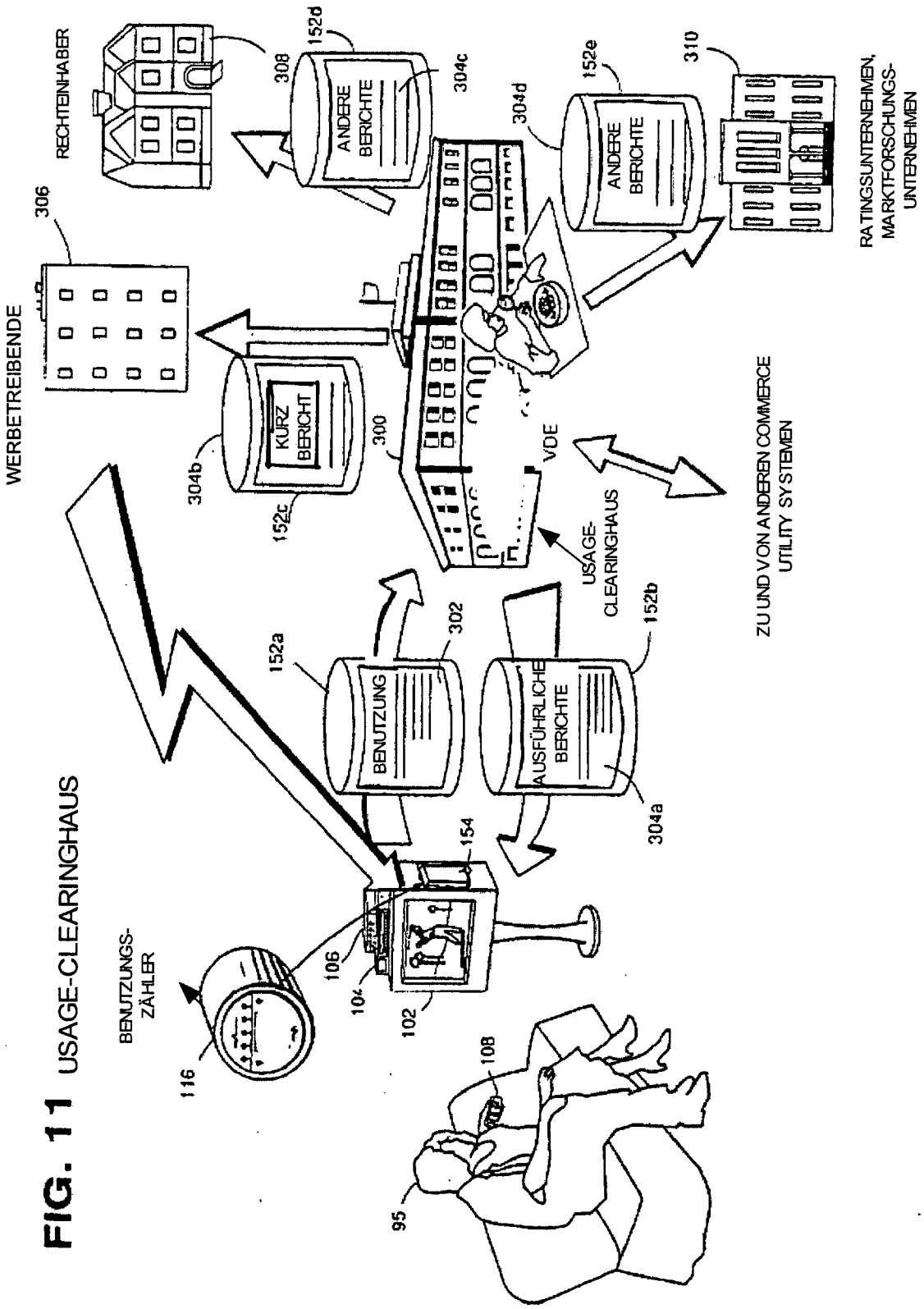


FIG. 11 USAGE-CLEARINGHAUS

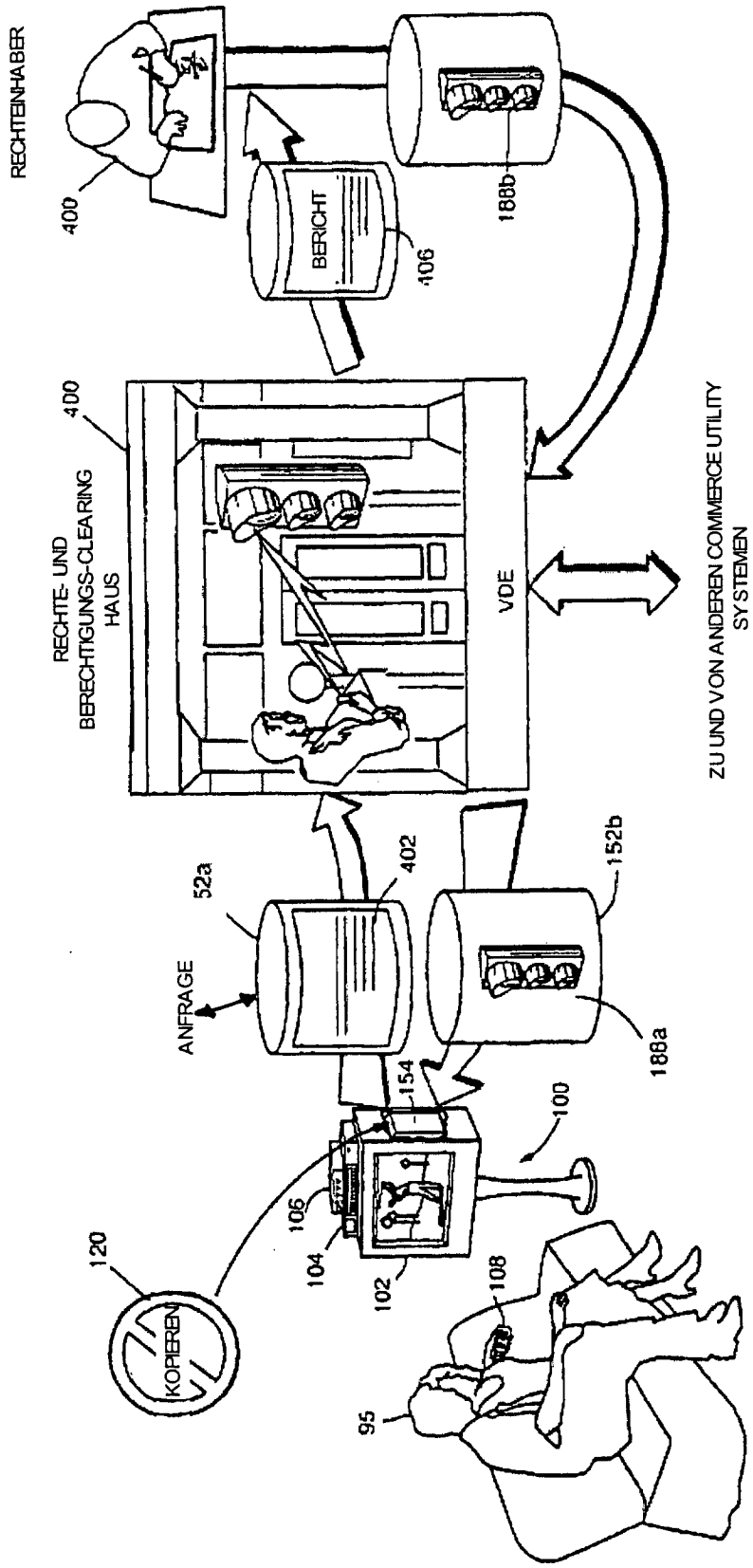


FIG. 12 RECHTE- UND BERECHTIGUNGS-CLEARINGHAUS

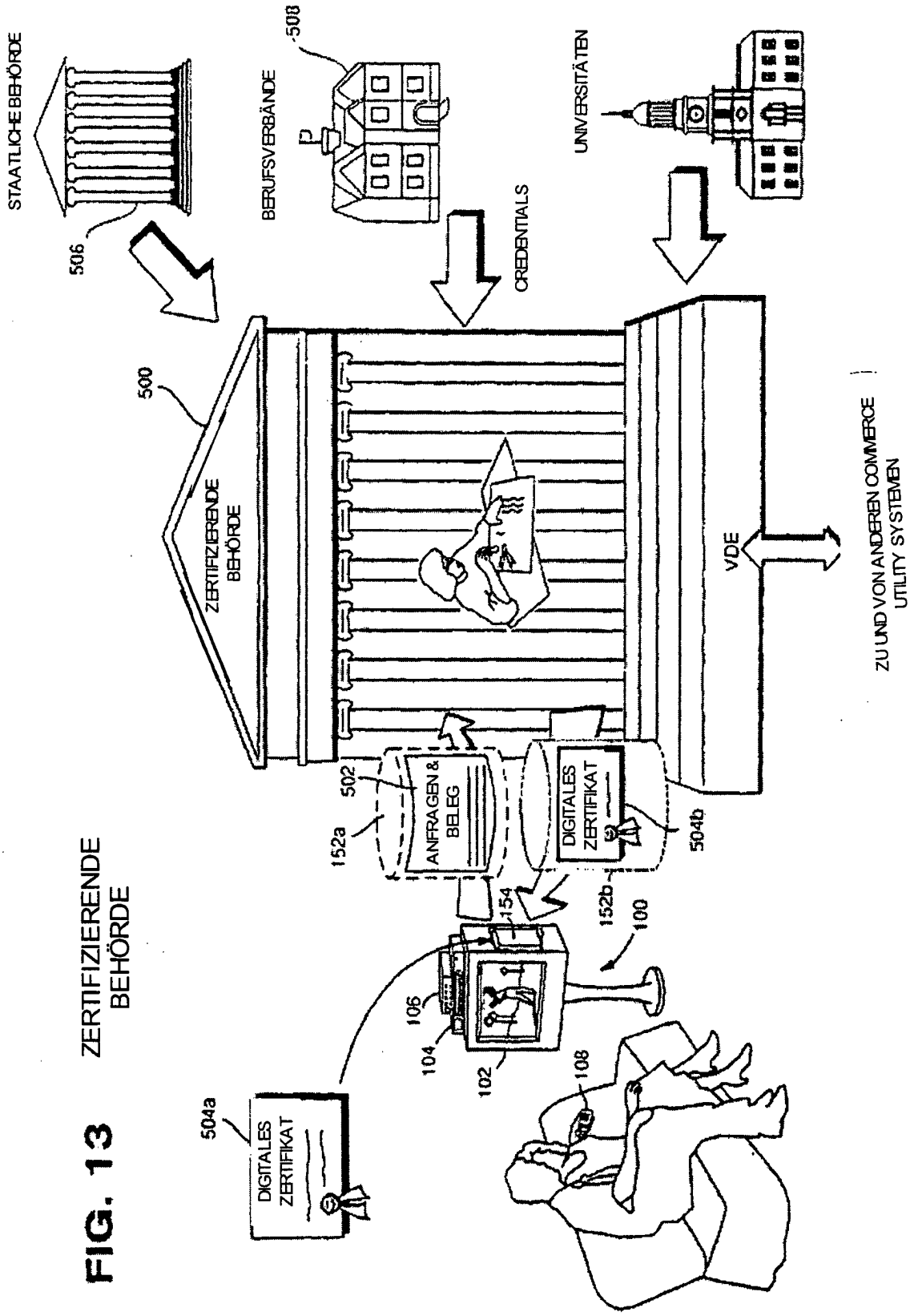


FIG. 13 ZERTIFIZIERENDE BEHÖRDE

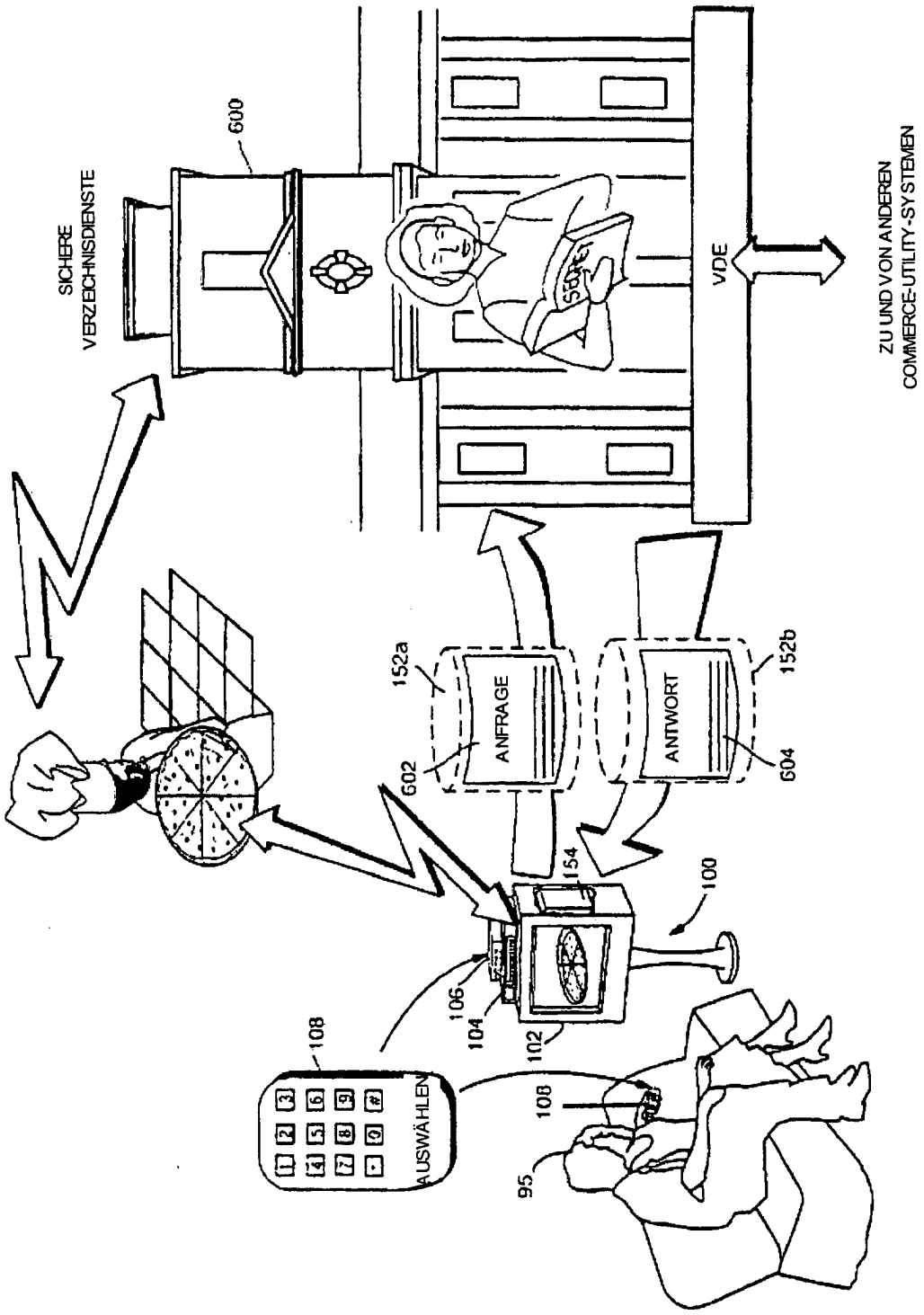


FIG. 14 SICHEREVERZEICHNISDIENSTE

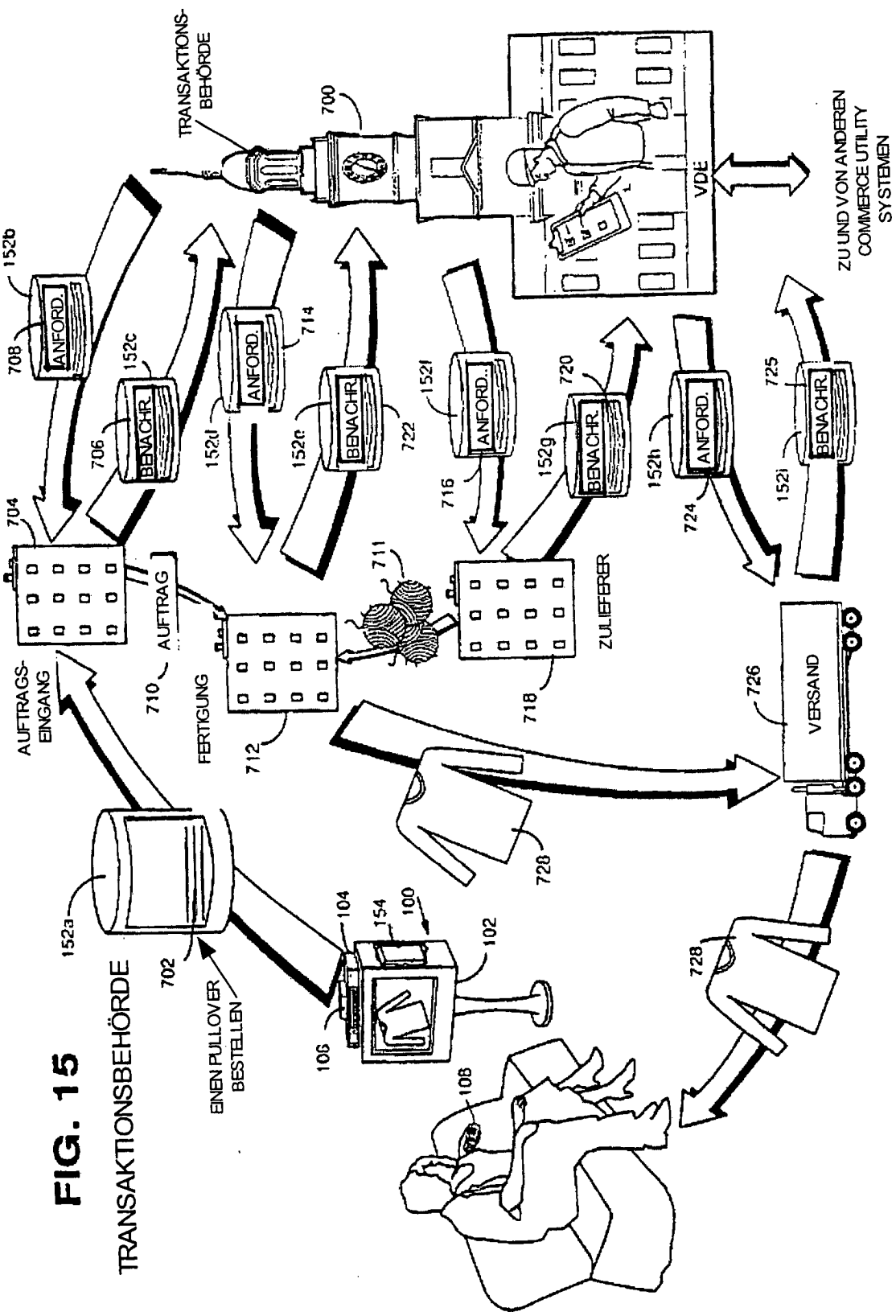


FIG. 15

TRANSAKTIONSBEHÖRDE

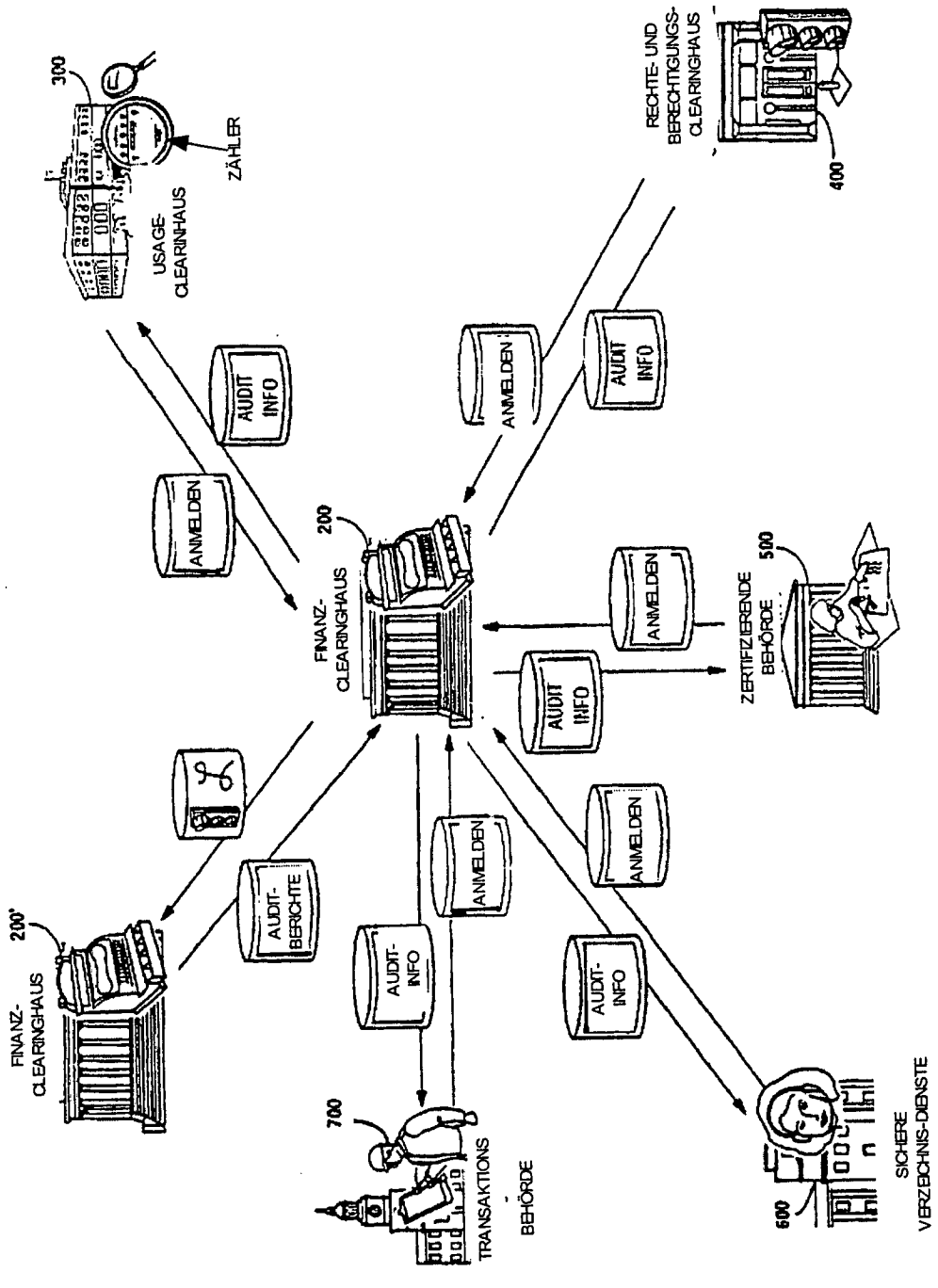

300
ZÄHLER
USAGE-CLEARINGHAUS
RECHTE- UND BERECHTIGUNGS-CLEARINGHAUS
400
AUDIT INFO
ANMELDEN
200
FINANZ-CLEARINGHAUS
ZERTIFIZIERENDE BEHÖRDE
500
AUDIT-BERICHTE
200'
FINANZ-CLEARINGHAUS
700
TRANSAKTIONS-BEHÖRDE
600
SICHERE VERZEICHNIS-DIENSTE

FIG. 16A

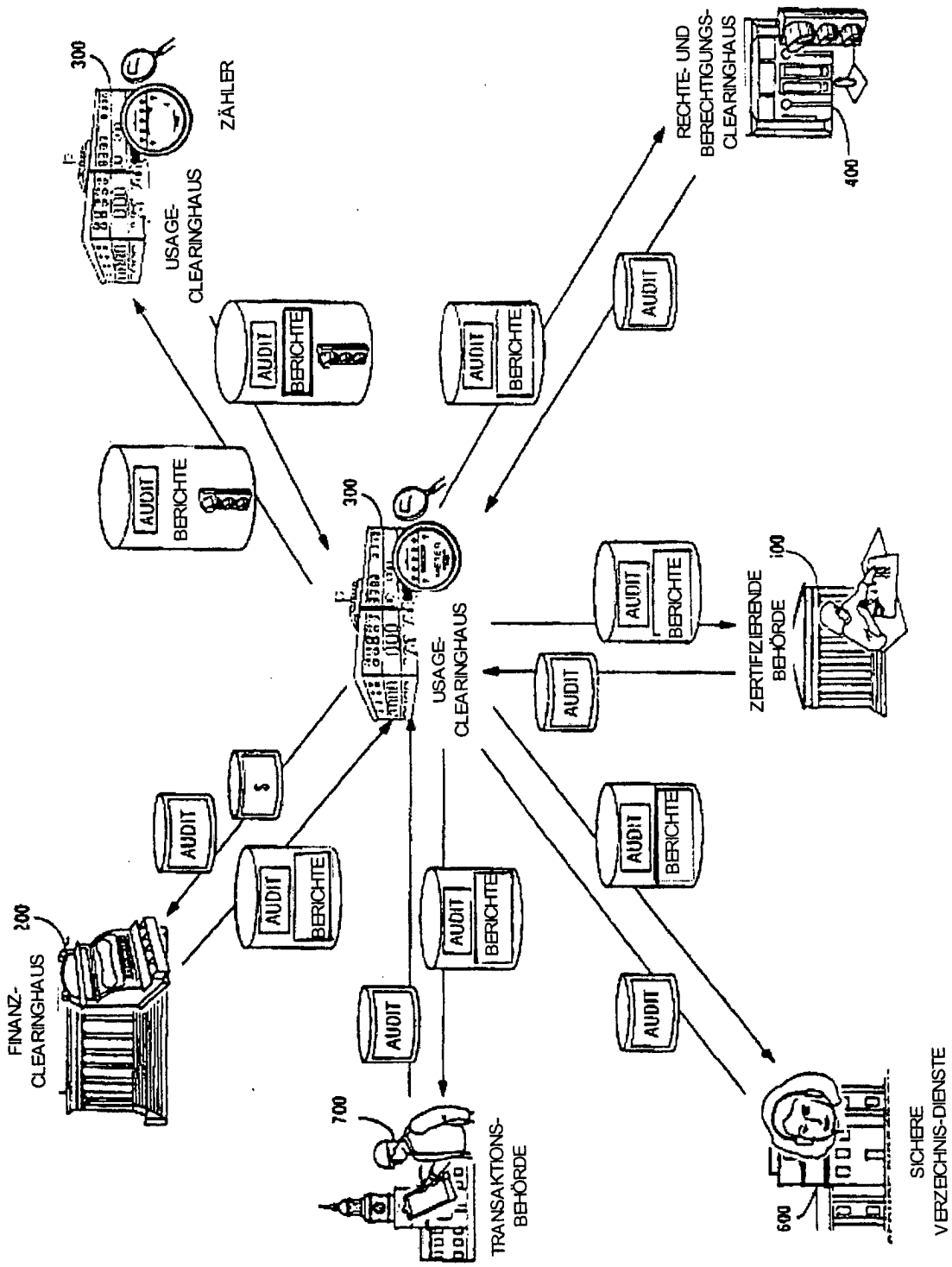
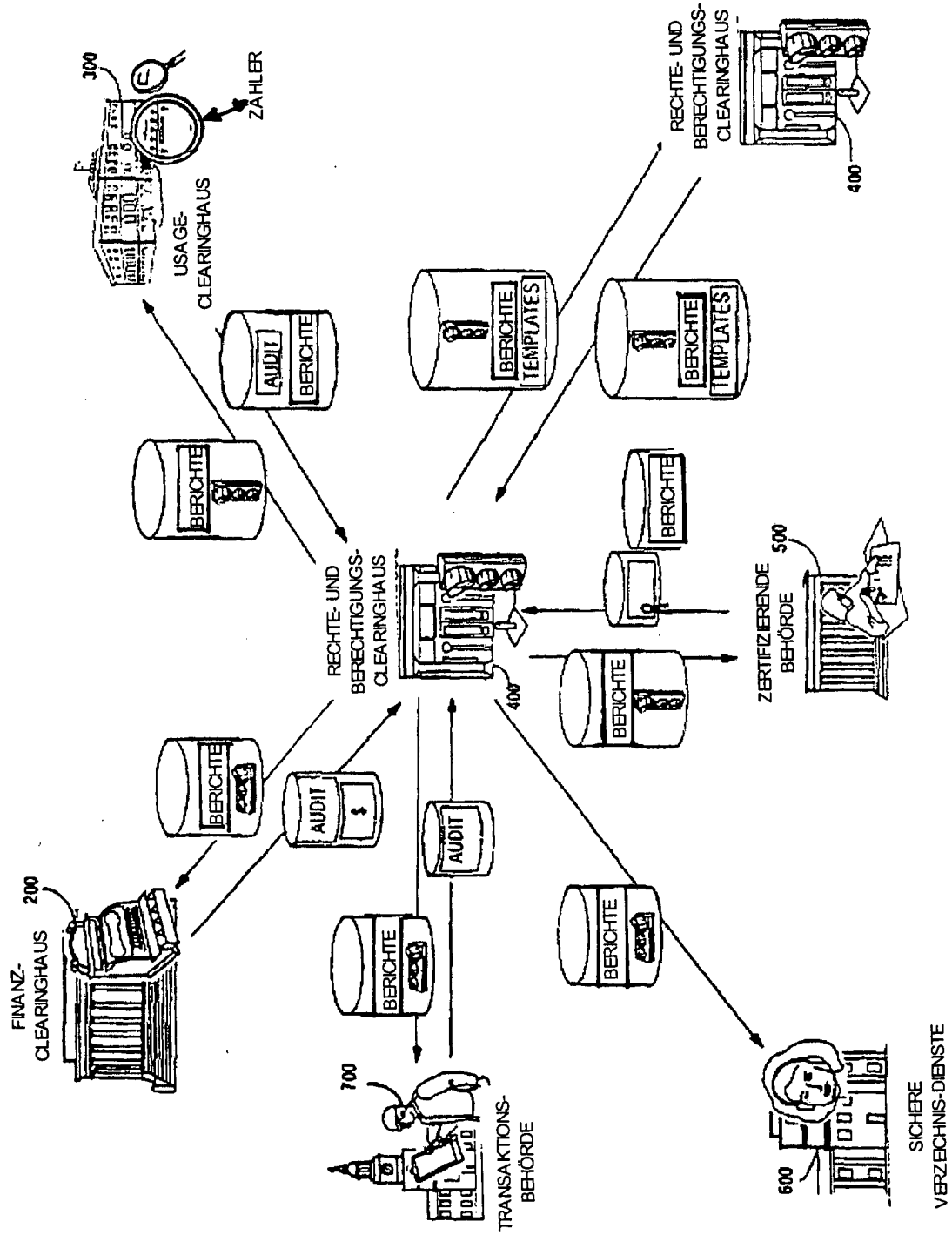

300
ZÄHLER
USAGE-
CLEARINGHAUS
AUDIT
BERICHTE
RECHTE- UND
BERECHTIGUNGS-
CLEARINGHAUS
400
ZERTIFIZIERENDE
BEHÖRDE
100
FINANZ-
CLEARINGHAUS
200
TRANSAKTIONS-
BEHÖRDE
700
SICHERE
VERZECHNIS-DIENSTE
600

FIG. 16B

FIG. 16C


300
ZÄHLER
USAGE-
CLEARINGHAUS
AUDIT
BERICHTE
BERICHTE
RECHTE- UND
BERECHTIGUNGS-
CLEARINGHAUS
BERICHTE
TEMPLATES
BERICHTE
TEMPLATES
RECHTE- UND
BERECHTIGUNGS-
CLEARINGHAUS
400
BERICHTE
BERICHTE
BERICHTE
ZERTIFIZIERENDE
BEHÖRDE
500
400
BERICHTE
AUDIT
AUDIT
200
FINANZ-
CLEARINGHAUS
BERICHTE
BERICHTE
700
TRANSAKTIONS-
BEHÖRDE
600
SICHERE
VERZEICHNIS-DIENSTE

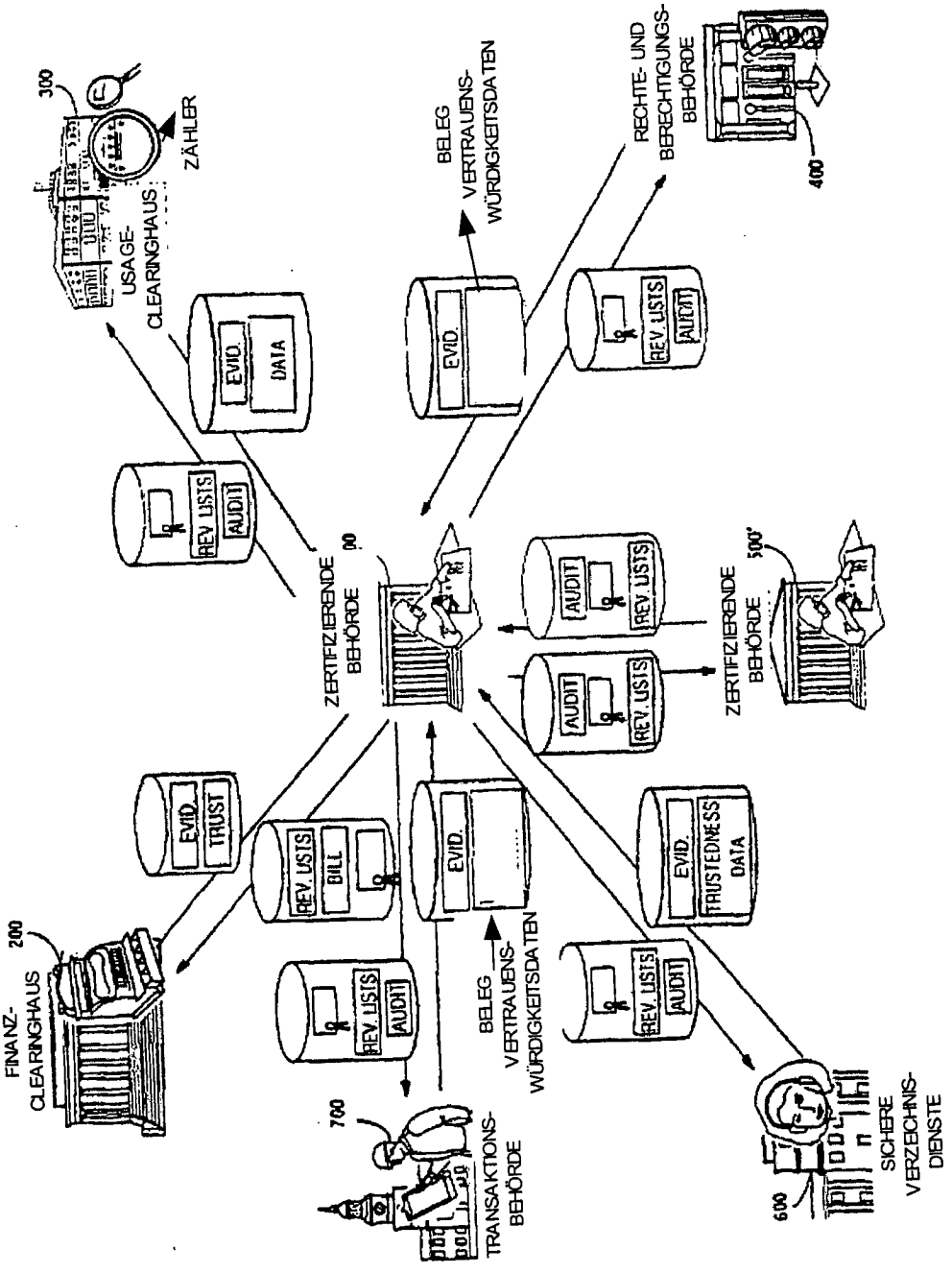

300
ZÄHLER
USAGE-
CLEARINGHAUS
EVID.
DATA
REV. LISTS
AUDIT
BELEG
VERTRAUENS-
WÜRDIGKEITSDATEN
EVID.
RECHTE- UND
BERECHTIGUNGS-
BEHÖRDE
400
REV. LISTS
AUDIT
ZERTIFIZIERENDE
BEHÖRDE
500
ZERTIFIZIERENDE
BEHÖRDE
500'
AUDIT
REV. LISTS
AUDIT
REV. LISTS
EVID.
TRUST
REV. LISTS
BILL
EVID.
EVID.
TRUSTEDNESS
DATA
200
FINANZ-
CLEARINGHAUS
REV. LISTS
AUDIT
BELEG
VERTRAUENS-
WÜRDIGKEITSDATEN
REV. LISTS
AUDIT
700
TRANSAKTIONS-
BEHÖRDE
600
SICHERE
VERZEICHNIS-
DIENSTE

FIG. 16D

FIG. 16E

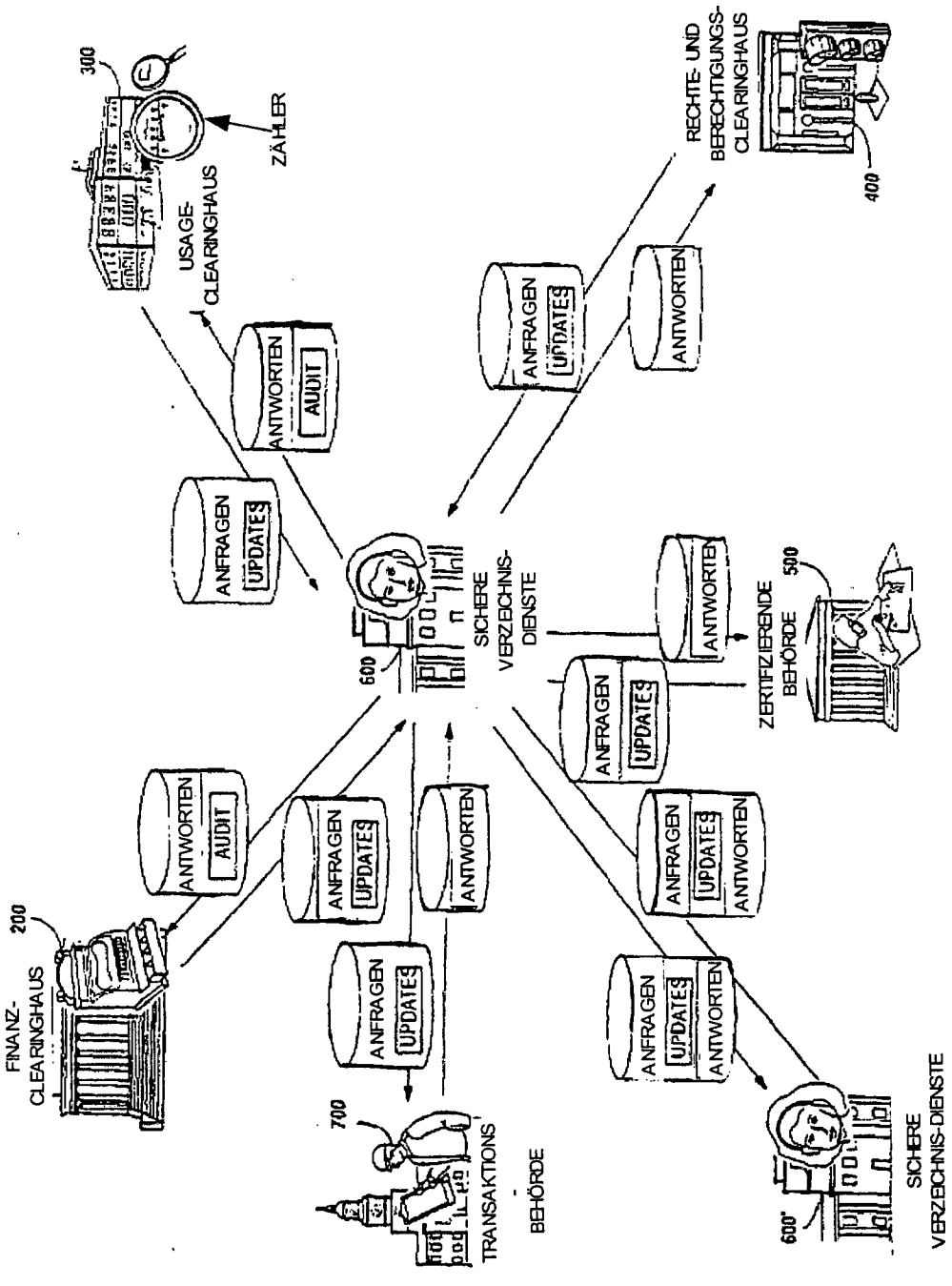
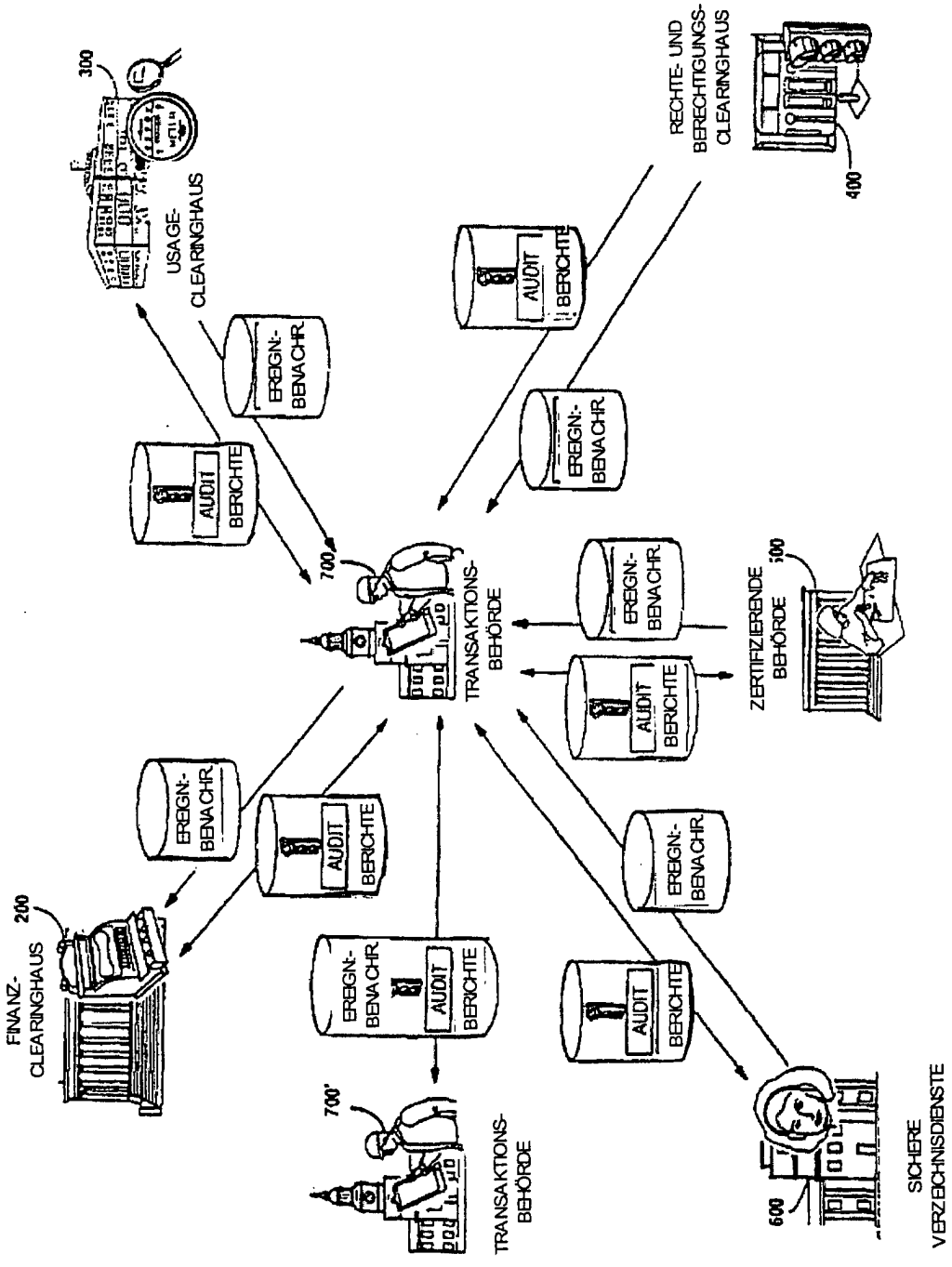

300
ZÄHLER
USAGE-CLEARINGHAUS
ANTWORTEN
AUDIT
ANFRAGEN
UPDATES
RECHTE- UND BERECHTIGUNGS-CLEARINGHAUS
400
600
SICHERE VERZEICHNIS-DIENSTE
500
ZERTIFIZIERENDE BEHÖRDE
200
FINANZ-CLEARINGHAUS
700
TRANSAKTIONS-BEHÖRDE
600'
SICHERE VERZEICHNIS-DIENSTE

FIG. 16F


300
USAGE-CLEARINGHAUS
RECHTE- UND BERECHTIGUNGS-CLEARINGHAUS
400
EREIGN-BENACHR
AUDIT
BERICHTE
700
TRANSAKTIONS-BEHÖRDE
ZERTIFIZIERENDE BEHÖRDE
500
200
FINANZ-CLEARINGHAUS
700'
TRANSAKTIONS-BEHÖRDE
600
SICHERE VERZEICHNISDIENSTE

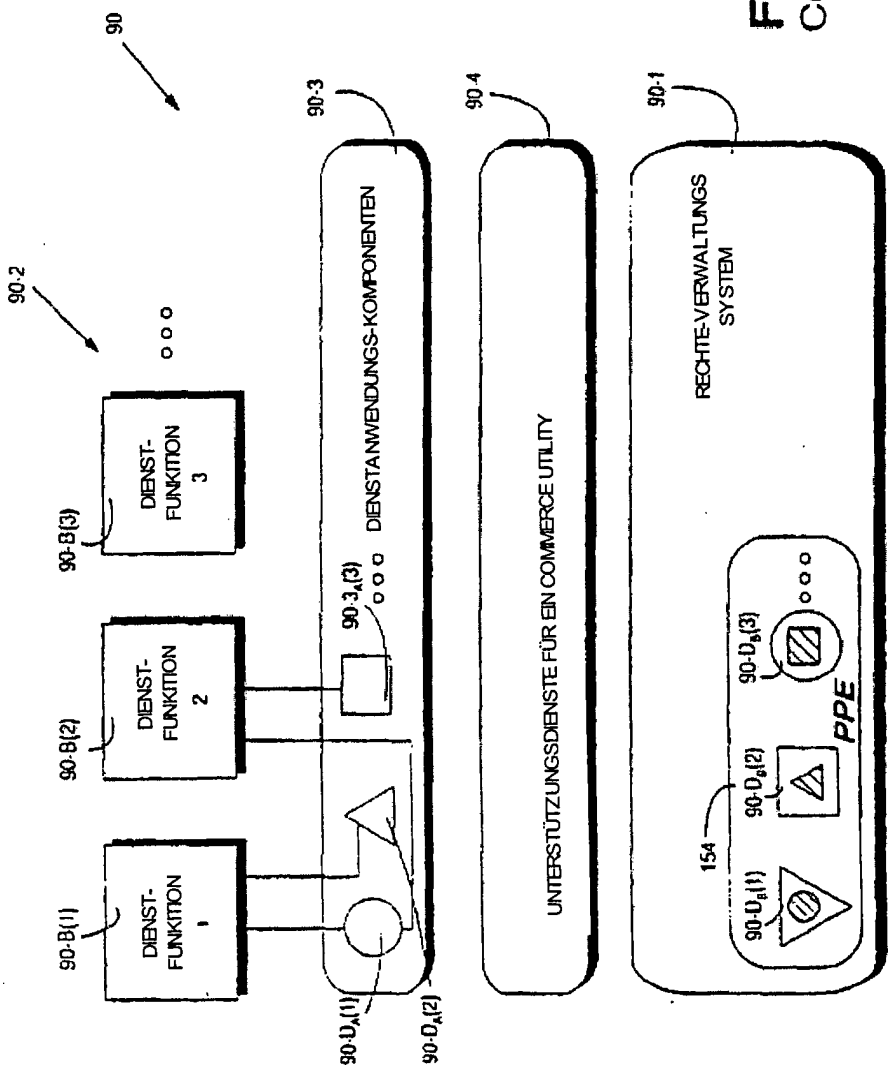


FIG. 17A
Commerce Utility System 90

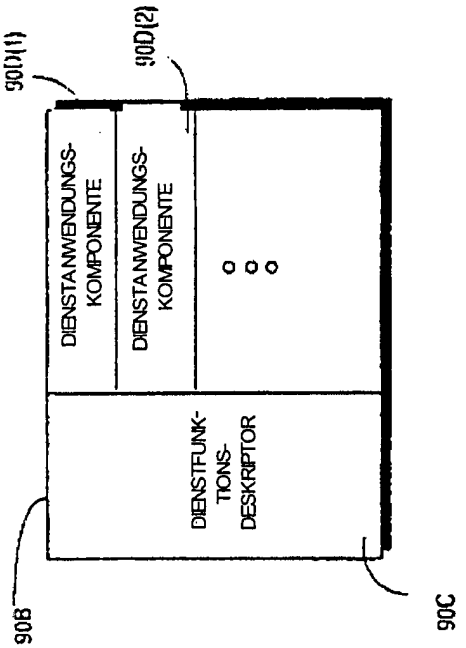


FIG. 17C

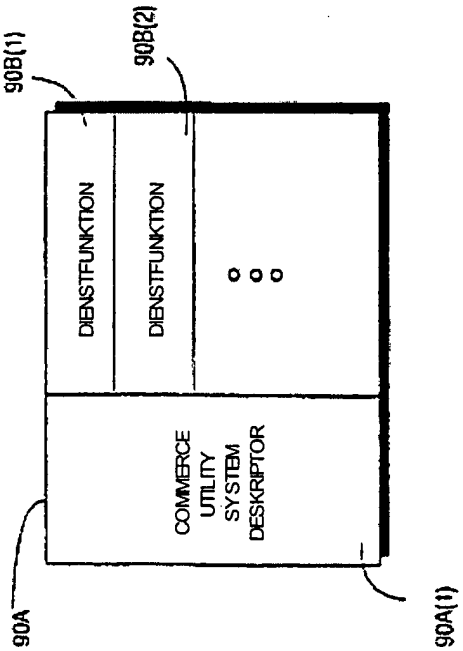


FIG. 17B

FIG. 17D-1

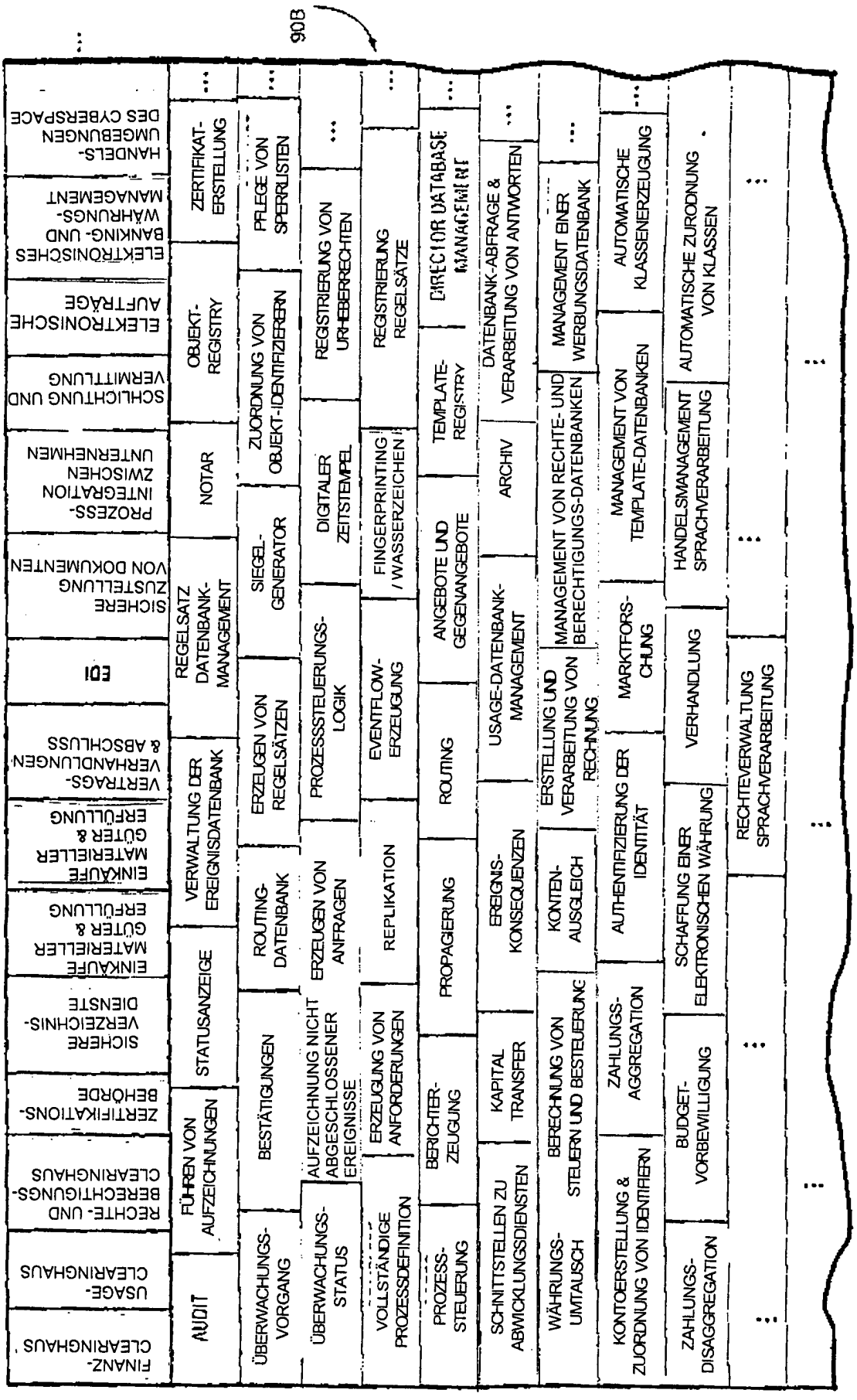

FINANZ-CLEARINGHAUS
USAGE-CLEARINGHAUS
RECHTE- UND BERECHTIGUNGS-CLEARINGHAUS
ZERTIFIKATIONS-BEHÖRDE
SICHERE VERZEICHNIS-DIENSTE
EINKÄUFE MATERIELLER GÜTER & ERFÜLLUNG
VERTRAGS-VERHANDLUNGEN & ABSCHLUSS
EDI
SICHERE ZUSTELLUNG VON DOKUMENTEN
PROZESS-INTEGRATION ZWISCHEN UNTERNEHMEN
SCHLICHTUNG UND VERMITTLUNG
ELEKTRONISCHE AUFTRÄGE
ELEKTRONISCHES BANKING- UND WÄHRUNGS-MANAGEMENT
HANDELS-UMGEBUNGEN DES CYBERSPACE
AUDIT
ÜBERWACHUNGS-VORGANG
ÜBERWACHUNGS-STATUS
VOLLSTÄNDIGE PROZESSDEFINITION
PROZESS-STEUERUNG
SCHNITTSTELLEN ZU ABWICKLUNGSDIENSTEN
WÄHRUNGS-UMTAUSCH
KONTOERSTELLUNG & ZUORDNUNG VON IDENTIFIERN
ZAHLUNGS-DISAGGREGATION
FÜHREN VON AUFZEICHNUNGEN
BESTÄTIGUNGEN
AUFZEICHNUNG NICHT ABGESCHLOSSENER EREIGNISSE
ERZEUGUNG VON ANFORDERUNGEN
BERICHTER-ZEUGUNG
KAPITAL TRANSFER
BERECHNUNG VON STEUERN UND BESTEUERUNG
ZAHLUNGS-AGGREGATION
BUDGET-VORBEWILLIGUNG
STATUSANZEIGE
ROUTING-DATENBANK
ERZEUGEN VON ANFRAGEN
REPLIKATION
PROPAGIERUNG
EREIGNIS-KONSEQUENZEN
KONTEN-AUSGLEICH
AUTHENTIFIZIERUNG DER IDENTITÄT
SCHAFFUNG EINER ELEKTRONISCHEN WÄHRUNG
VERWALTUNG DER EREIGNISDATENBANK
ERZEUGEN VON REGELSÄTZEN
PROZESSSTEUERUNGS-LOGIK
EVENTFLOW-ERZEUGUNG
ROUTING
ERSTELLUNG UND VERARBEITUNG VON RECHNUNG
MARKTFORS-CHUNG
VERHANDLUNG
RECHTEVERWALTUNG
SPRACHVERARBEITUNG
REGELSATZ DATENBANK-MANAGEMENT
SIEGEL-GENERATOR
DIGITALER ZEITSTEMPEL
FINGERPRINTING / WASSERZEICHEN
ANGEBOTE UND GEGENANGEBOTE
USAGE-DATENBANK-MANAGEMENT
MANAGEMENT VON RECHTE- UND BERECHTIGUNGS-DATENBANKEN
MANAGEMENT VON TEMPLATE-DATENBANKEN
HANDELSMANAGEMENT SPRACHVERARBEITUNG
NOTAR
ZUORDNUNG VON OBJEKT-IDENTIFIERN
REGISTRIERUNG VON URHEBERRECHTEN
REGISTRIERUNG REGELSÄTZE
TEMPLATE-REGISTRY
ARCHIV
DATENBANK-ABFRAGE & VERARBEITUNG VON ANTWORTEN
MANAGEMENT EINER WERBUNGSDATENBANK
AUTOMATISCHE KLASSENERZEUGUNG
AUTOMATISCHE ZUORDNUNG VON KLASSEN
OBJEKT-REGISTRY
PFLEGE VON SPERRLISTEN
ZERTIFIKAT-ERSTELLUNG
908

FIG. 17D-2

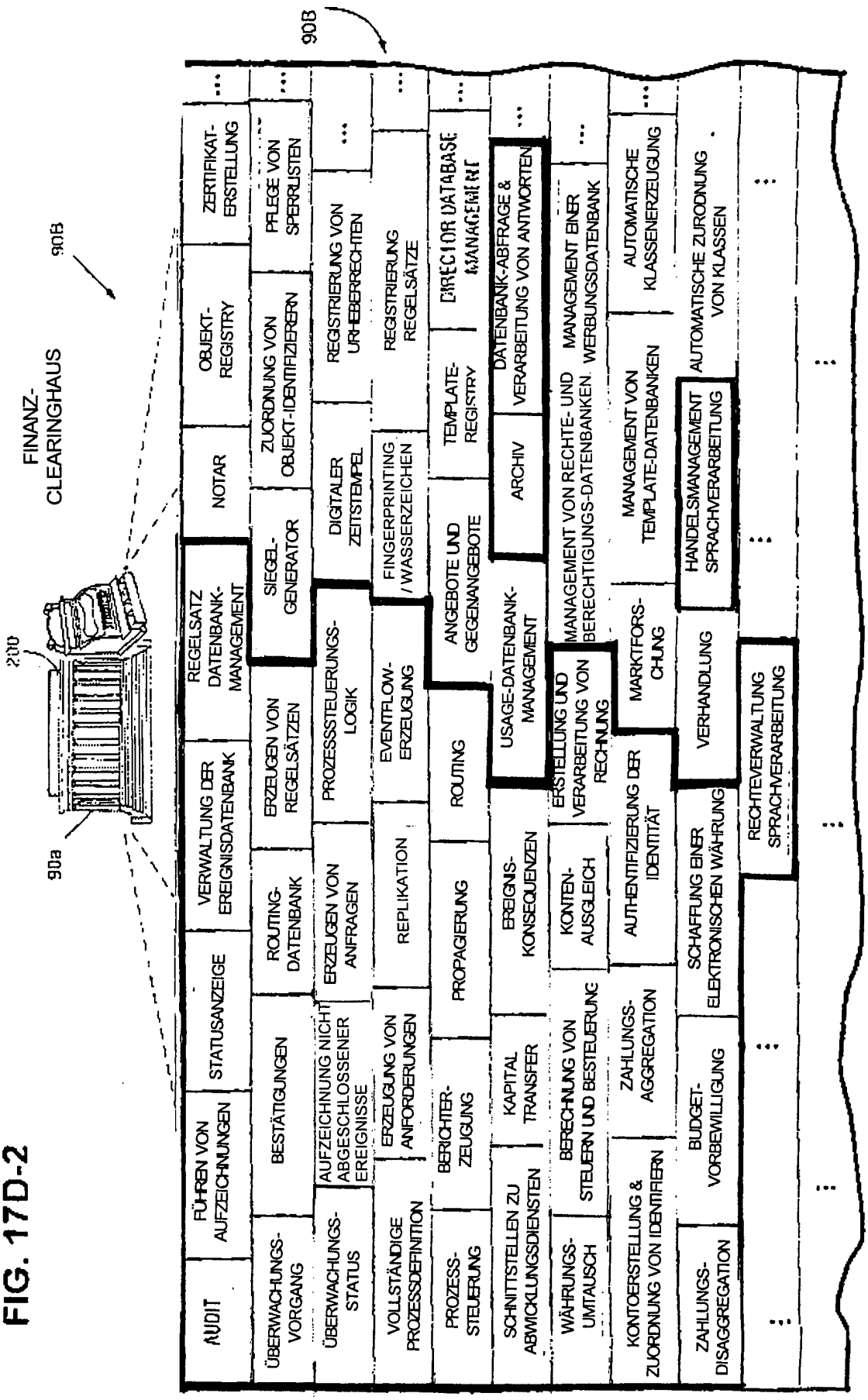
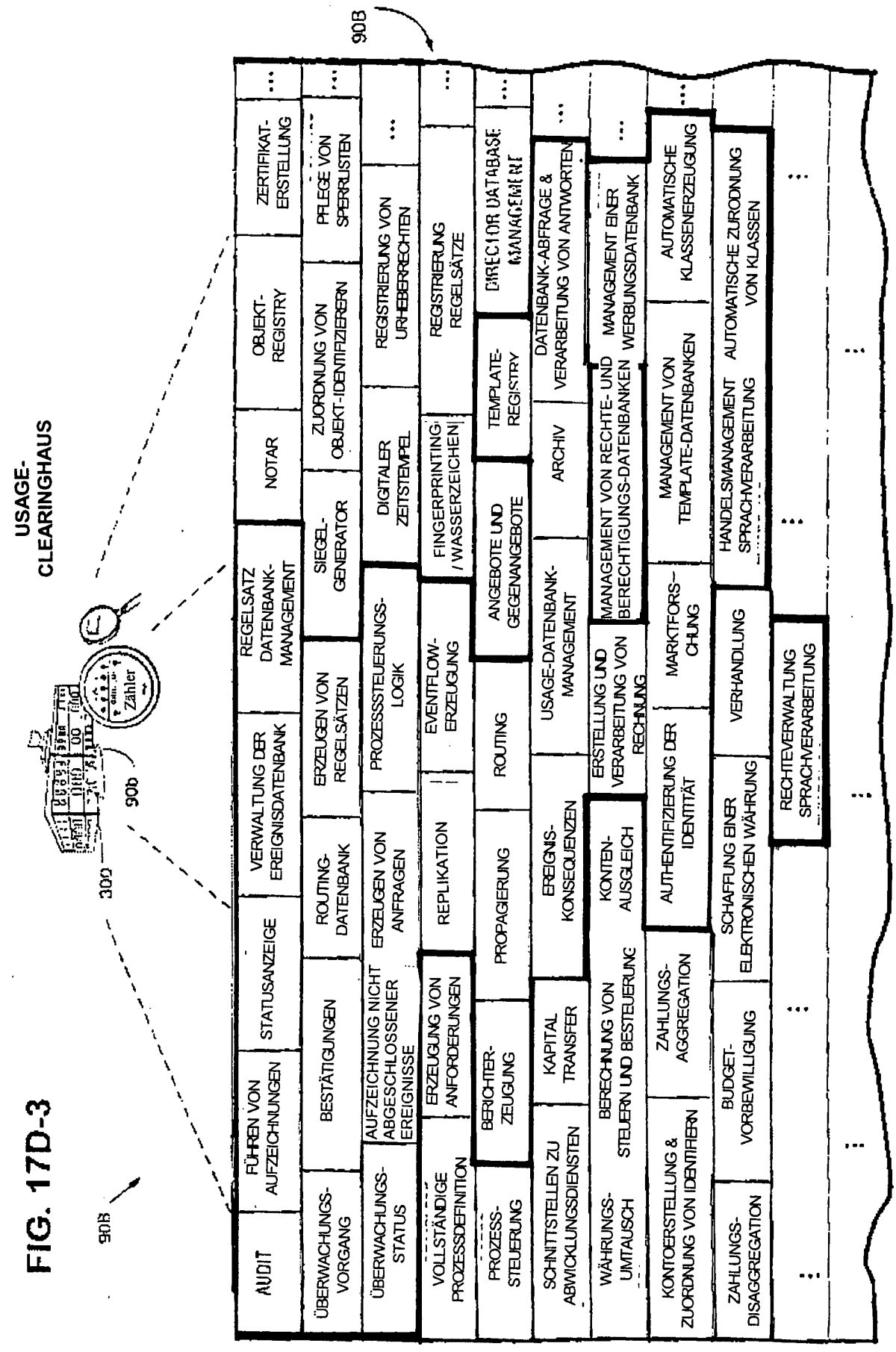

FINANZ-
CLEARINGHAUS
200
90a
90b
90b
AUDIT
FÜHREN VON AUFZEICHNUNGEN
STATUSANZEIGE
VERWALTUNG DER EREIGNISDATENBANK
REGELSATZ DATENBANK-MANAGEMENT
NOTAR
OBJEKT-REGISTRY
ZERTIFIKAT-ERSTELLUNG
ÜBERWACHUNGS-VORGANG
BESTÄTIGUNGEN
ROUTING-DATENBANK
ERZEUGEN VON REGELSÄTZEN
SIEGEL-GENERATOR
ZUORDNUNG VON OBJEKT-IDENTIFIZIERERN
PFLEGE VON SPERRLISTEN
ÜBERWACHUNGS-STATUS
AUFZEICHNUNG NICHT ABGESCHLOSSENER EREIGNISSE
ERZEUGEN VON ANFRAGEN
PROZESSSTEUERUNGS-LOGIK
DIGITALER ZEITSTEMPEL
REGISTRIERUNG VON URHEBERRECHTEN
VOLLSTÄNDIGE PROZESSDEFINITION
ERZEUGUNG VON ANFORDERUNGEN
REPLIKATION
EVENTFLOW-ERZEUGUNG
FINGERPRINTING /WASSERZEICHEN
REGISTRIERUNG REGELSÄTZE
PROZESS-STEUERUNG
BERICHTER-ZEUGUNG
PROPAGIERUNG
ROUTING
ANGEBOTE UND GEGENANGEBOTE
TEMPLATE-REGISTRY
DIRECTOR DATABASE MANAGEMENT
SCHNITTSTELLEN ZU ABWICKLUNGSDIENSTEN
KAPITAL TRANSFER
EREIGNIS-KONSEQUENZEN
USAGE-DATENBANK-MANAGEMENT
ARCHIV
DATENBANK-ABFRAGE & VERARBEITUNG VON ANTWORTEN
WÄHRUNGS-UMTAUSCH
BERECHNUNG VON STEUERN UND BESTEUERUNG
KONTEN-AUSGLEICH
ERSTELLUNG UND VERARBEITUNG VON RECHNUNG
MANAGEMENT VON RECHTE- UND BERECHTIGUNGS-DATENBANKEN
MANAGEMENT EINER WERBUNGSDATENBANK
KONTOERSTELLUNG & ZUORDNUNG VON IDENTIFIERN
ZAHLUNGS-AGGREGATION
AUTHENTIFIZIERUNG DER IDENTITÄT
MARKTFORS-CHUNG
MANAGEMENT VON TEMPLATE-DATENBANKEN
AUTOMATISCHE KLASSENERZEUGUNG
ZAHLUNGS-DISAGGREGATION
BUDGET-VORBEWILLIGUNG
SCHAFFUNG EINER ELEKTRONISCHEN WÄHRUNG
VERHANDLUNG
HANDELSMANAGEMENT SPRACHVERARBEITUNG
AUTOMATISCHE ZUORDNUNG VON KLASSEN
RECHTEVERWALTUNG SPRACHVERARBEITUNG

FIG. 17D-3


USAGE-CLEARINGHAUS
90B
300
90b
Zähler
AUDIT
FÜHREN VON AUFZEICHNUNGEN
STATUSANZEIGE
VERWALTUNG DER EREIGNISDATENBANK
REGELSATZ DATENBANK-MANAGEMENT
NOTAR
OBJEKT-REGISTRY
ZERTIFIKAT-ERSTELLUNG
ÜBERWACHUNGS-VORGANG
BESTÄTIGUNGEN
ROUTING-DATENBANK
ERZEUGEN VON REGELSÄTZEN
SIEGEL-GENERATOR
ZUORDNUNG VON OBJEKT-IDENTIFIZIERERN
PFLEGE VON SPERRLISTEN
ÜBERWACHUNGS-STATUS
AUFZEICHNUNG NICHT ABGESCHLOSSENER EREIGNISSE
ERZEUGEN VON ANFRAGEN
PROZESSSTEUERUNGS-LOGIK
DIGITALER ZEITSTEMPEL
REGISTRIERUNG VON URHEBERRECHTEN
VOLLSTÄNDIGE PROZESSDEFINITION
ERZEUGUNG VON ANFORDERUNGEN
REPLIKATION
EVENTFLOW-ERZEUGUNG
FINGERPRINTING / WASSERZEICHEN
REGISTRIERUNG REGELSÄTZE
PROZESS-STEUERUNG
BERICHTER-ZEUGUNG
PROPAGIERUNG
ROUTING
ANGEBOTE UND GEGENANGEBOTE
TEMPLATE-REGISTRY
DIRECTOR DATABASE MANAGEMENT
SCHNITTSTELLEN ZU ABWICKLUNGSDIENSTEN
KAPITAL TRANSFER
EREIGNIS-KONSEQUENZEN
USAGE-DATENBANK-MANAGEMENT
ARCHIV
DATENBANK-ABFRAGE & VERARBEITUNG VON ANTWORTEN
WÄHRUNGS-UMTAUSCH
BERECHNUNG VON STEUERN UND BESTEUERUNG
KONTEN-AUSGLEICH
ERSTELLUNG UND VERARBEITUNG VON RECHNUNG
MANAGEMENT VON RECHTE- UND BERECHTIGUNGS-DATENBANKEN
MANAGEMENT EINER WERBUNGSDATENBANK
KONTOERSTELLUNG & ZUORDNUNG VON IDENTIFIERN
ZAHLUNGS-AGGREGATION
AUTHENTIFIZIERUNG DER IDENTITÄT
MARKTFORS-CHUNG
MANAGEMENT VON TEMPLATE-DATENBANKEN
AUTOMATISCHE KLASSENERZEUGUNG
ZAHLUNGS-DISAGGREGATION
BUDGET-VORBEWILLIGUNG
SCHAFFUNG EINER ELEKTRONISCHEN WÄHRUNG
VERHANDLUNG
HANDELSMANAGEMENT SPRACHVERARBEITUNG
AUTOMATISCHE ZUORDNUNG VON KLASSEN
RECHTEVERWALTUNG SPRACHVERARBEITUNG

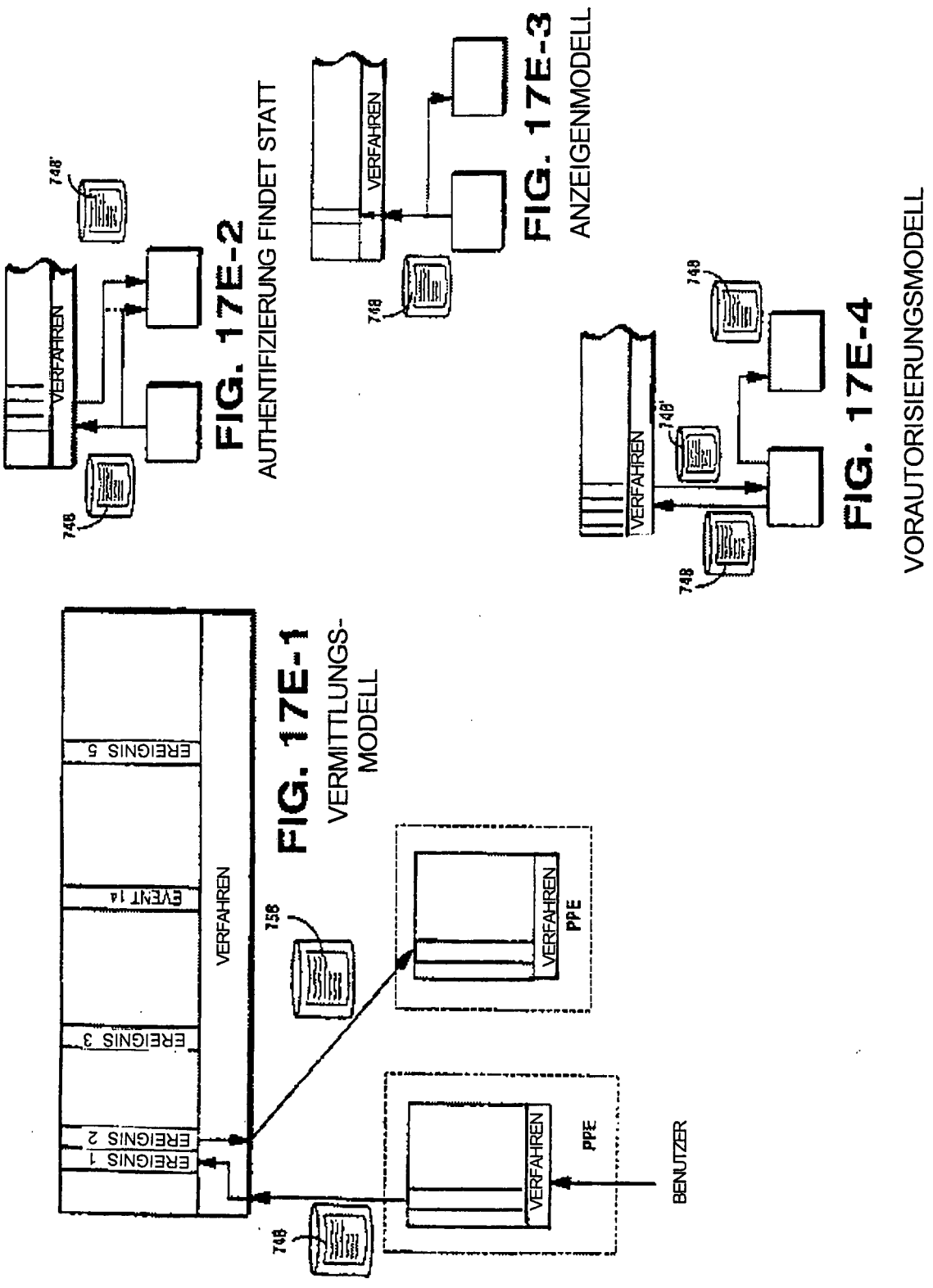


FIG. 17E-2
AUTHENTIFIZIERUNG FINDET STATT

FIG. 17E-3
ANZEIGENMODELL

FIG. 17E-4
VORAUTORISIERUNGSMODELL

FIG. 17E-1
VERMITTLUNGS-
MODELL

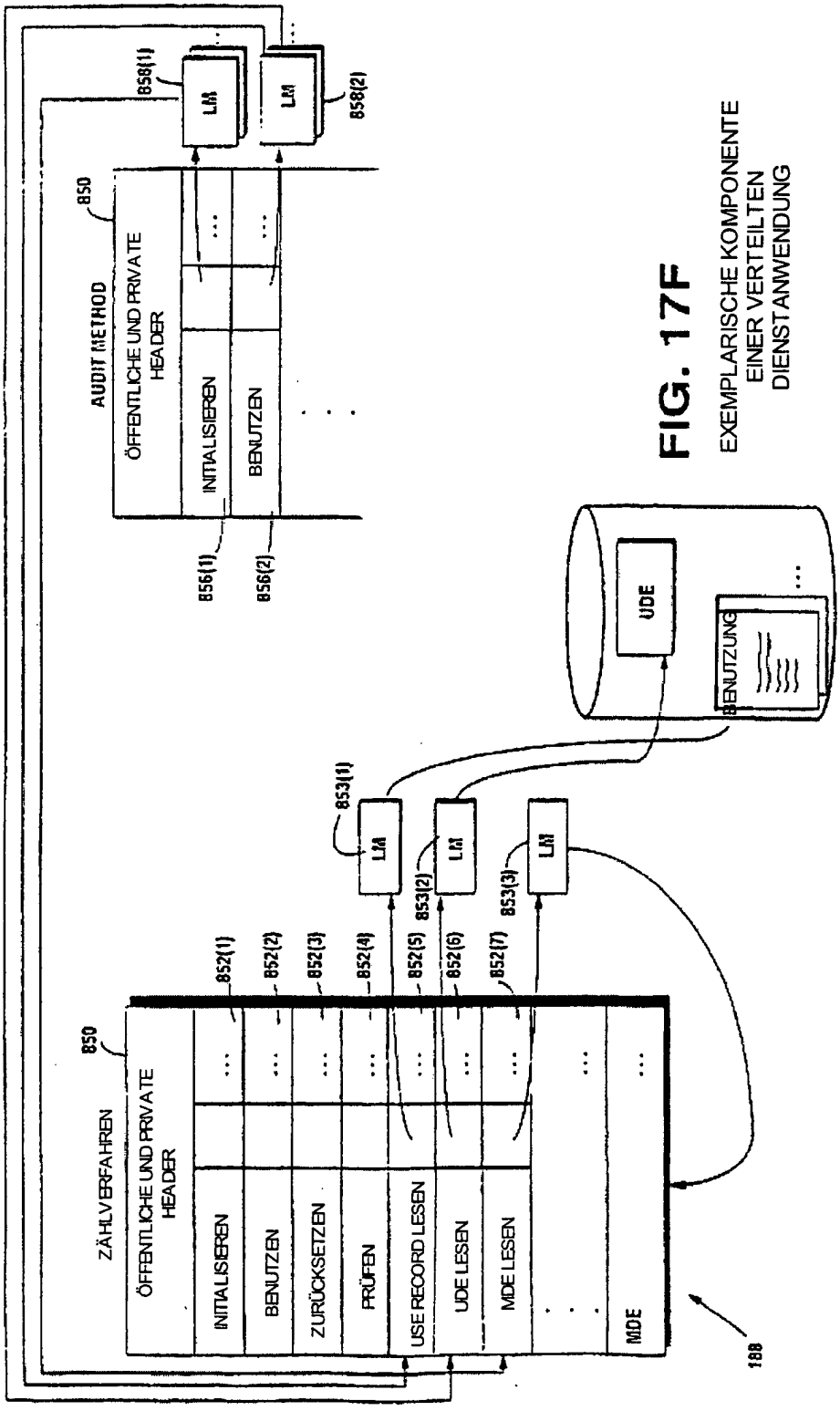


FIG. 17F

EXEMPLARISCHE KOMPONENTE EINER VERTEILTEN DIENSTANWENDUNG

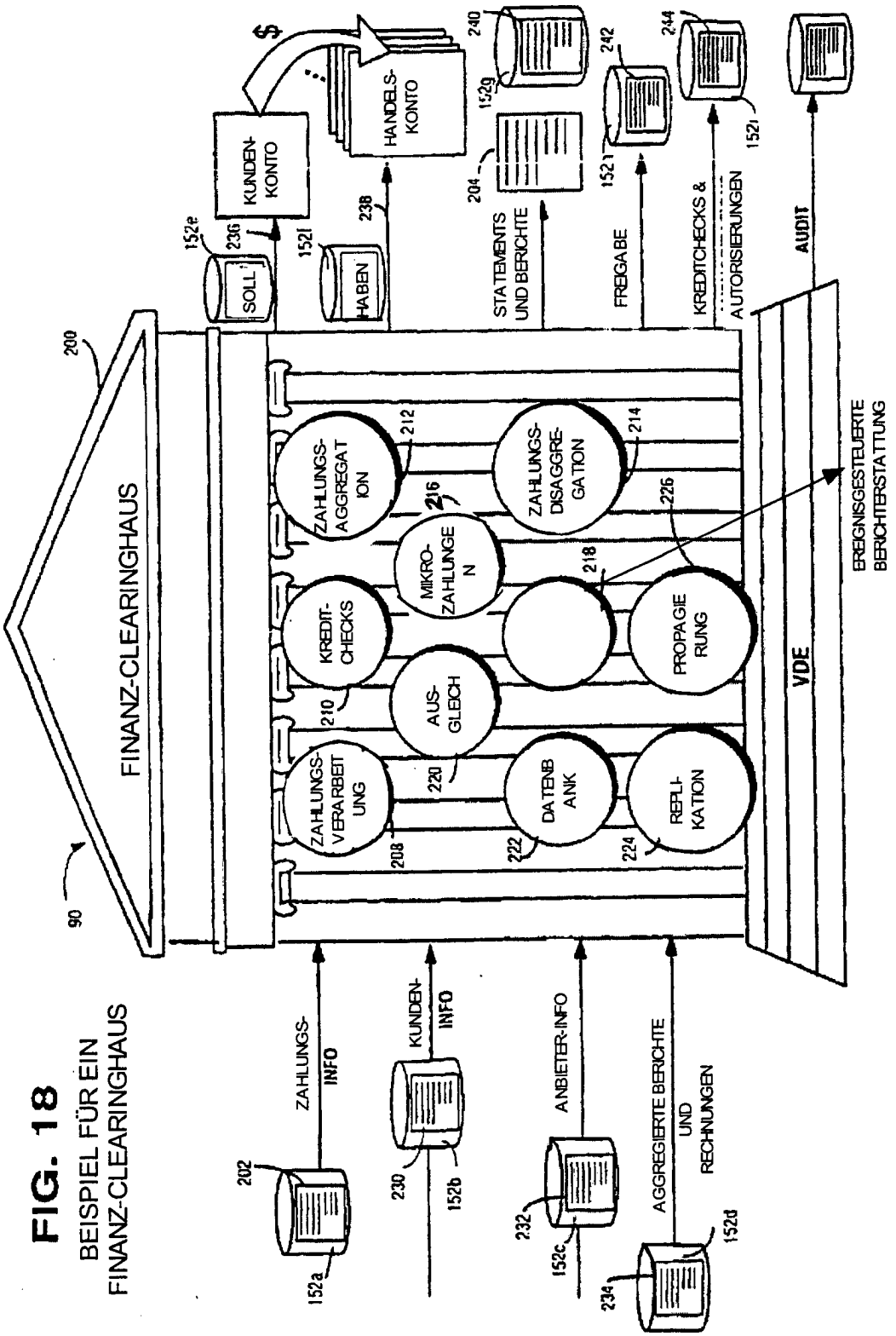


FIG. 18
BEISPIEL FÜR EIN FINANZ-CLEARINGHAUS

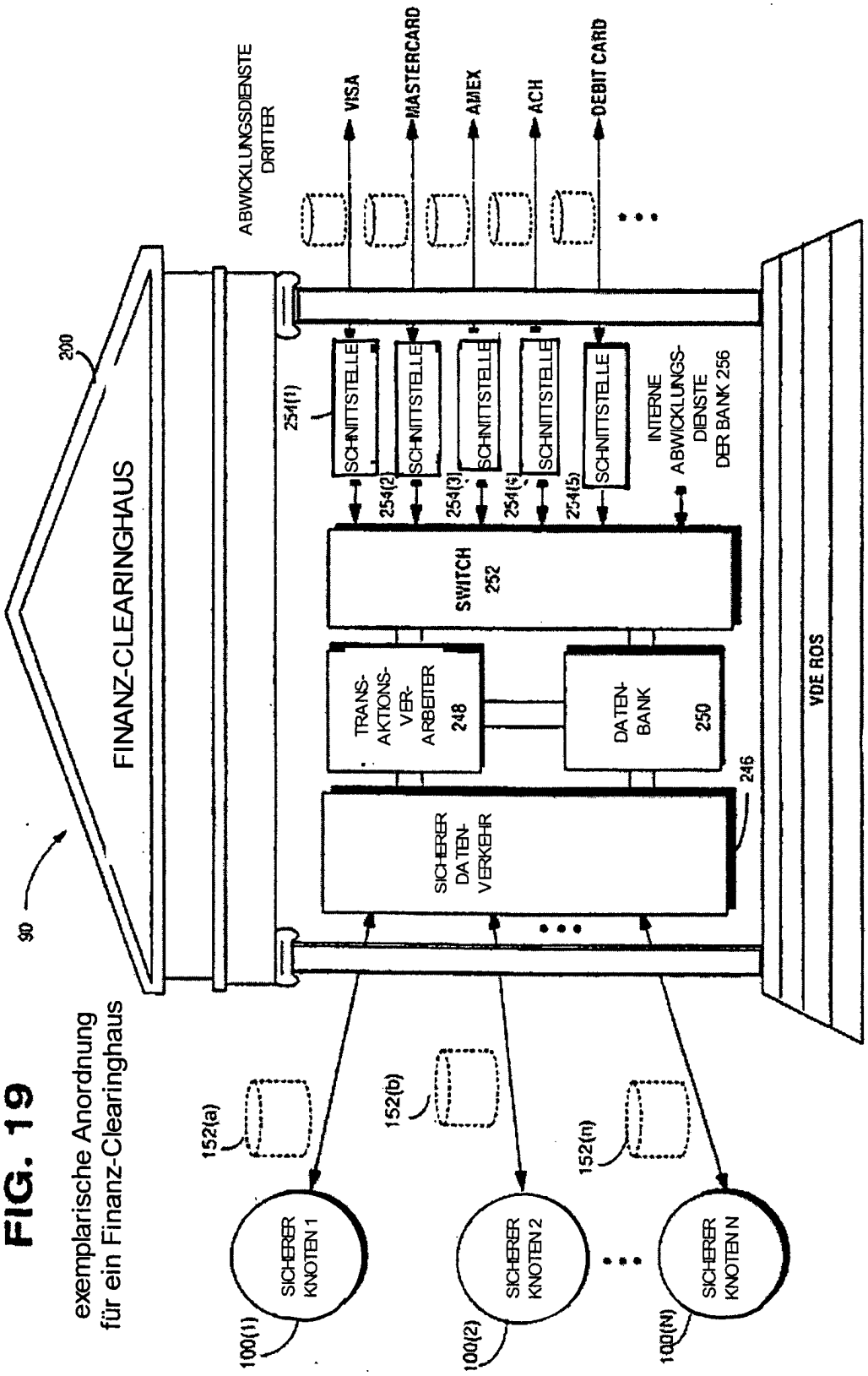


FIG. 19

exemplarische Anordnung für ein Finanz-Clearinghaus

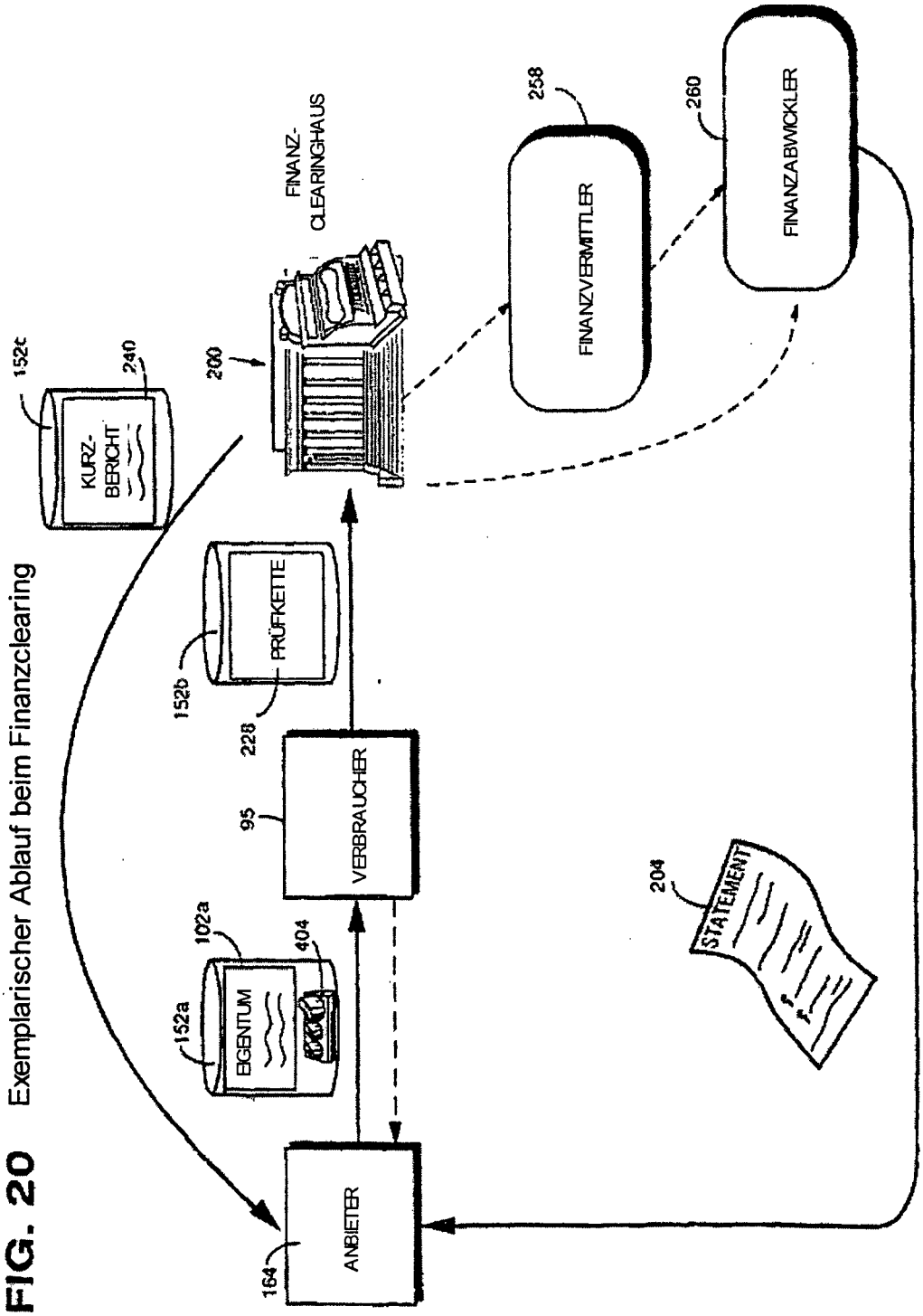


FIG. 20 Exemplarischer Ablauf beim Finanzclearing

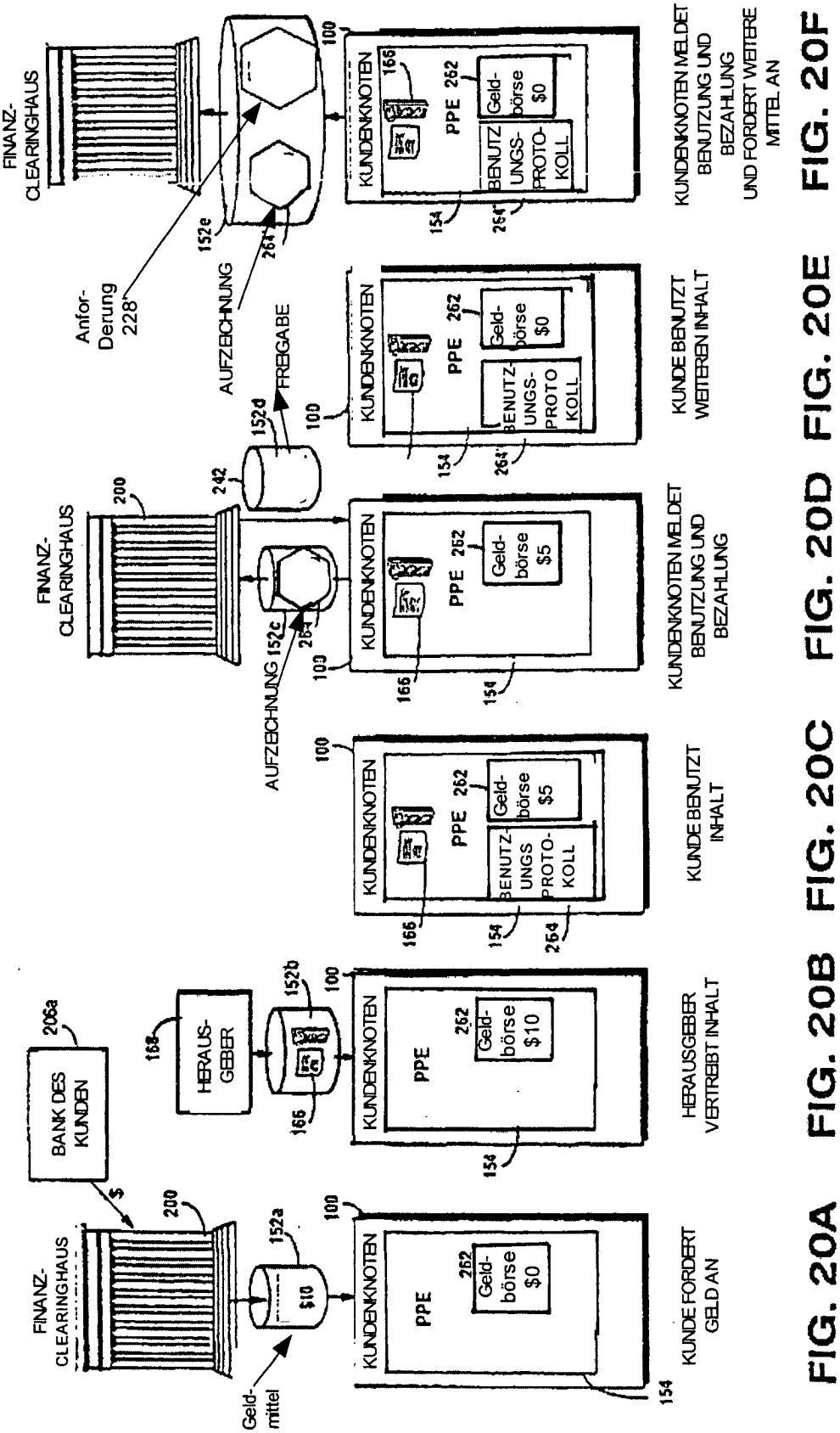


FIG. 20A FIG. 20B FIG. 20C FIG. 20D FIG. 20E FIG. 20F

Beispiel für Aktivitäten des Finanzclearing

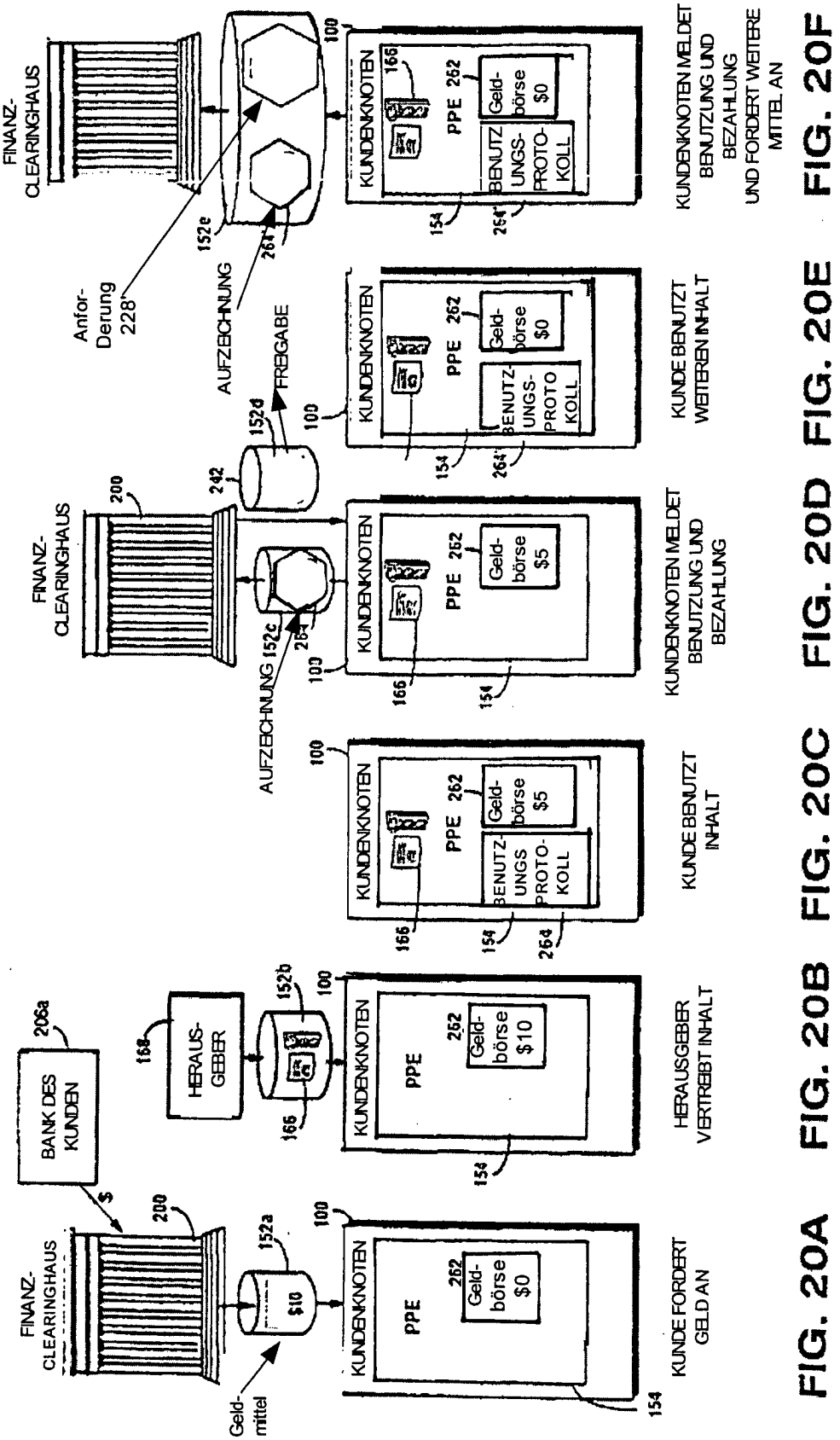


FIG. 20A FIG. 20B FIG. 20C FIG. 20D FIG. 20E FIG. 20F

Beispiel für Aktivitäten des Finanzclearing

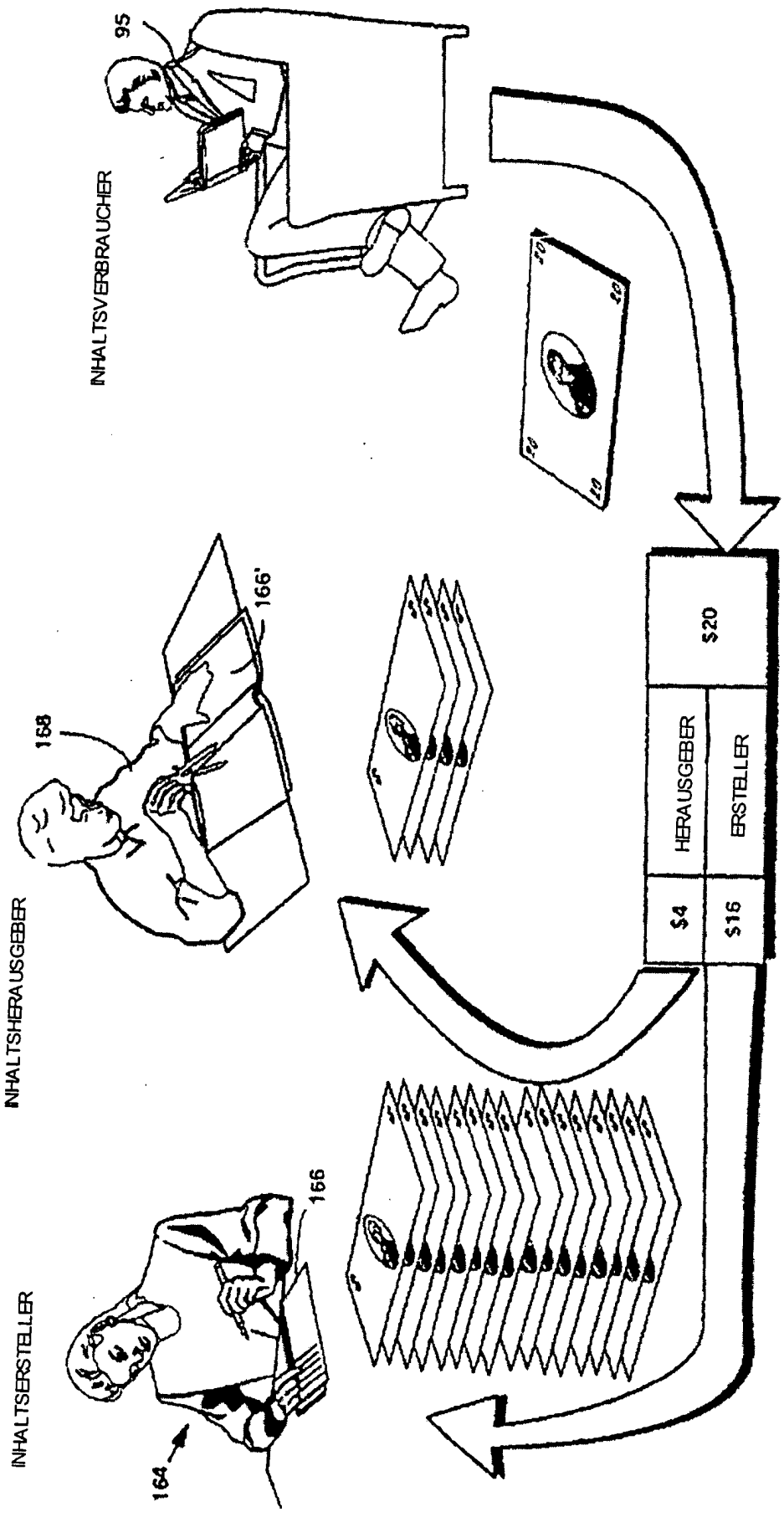


FIG. 21
BEISPIEL FÜR
ZAHLUNGSDISAGGREGATION

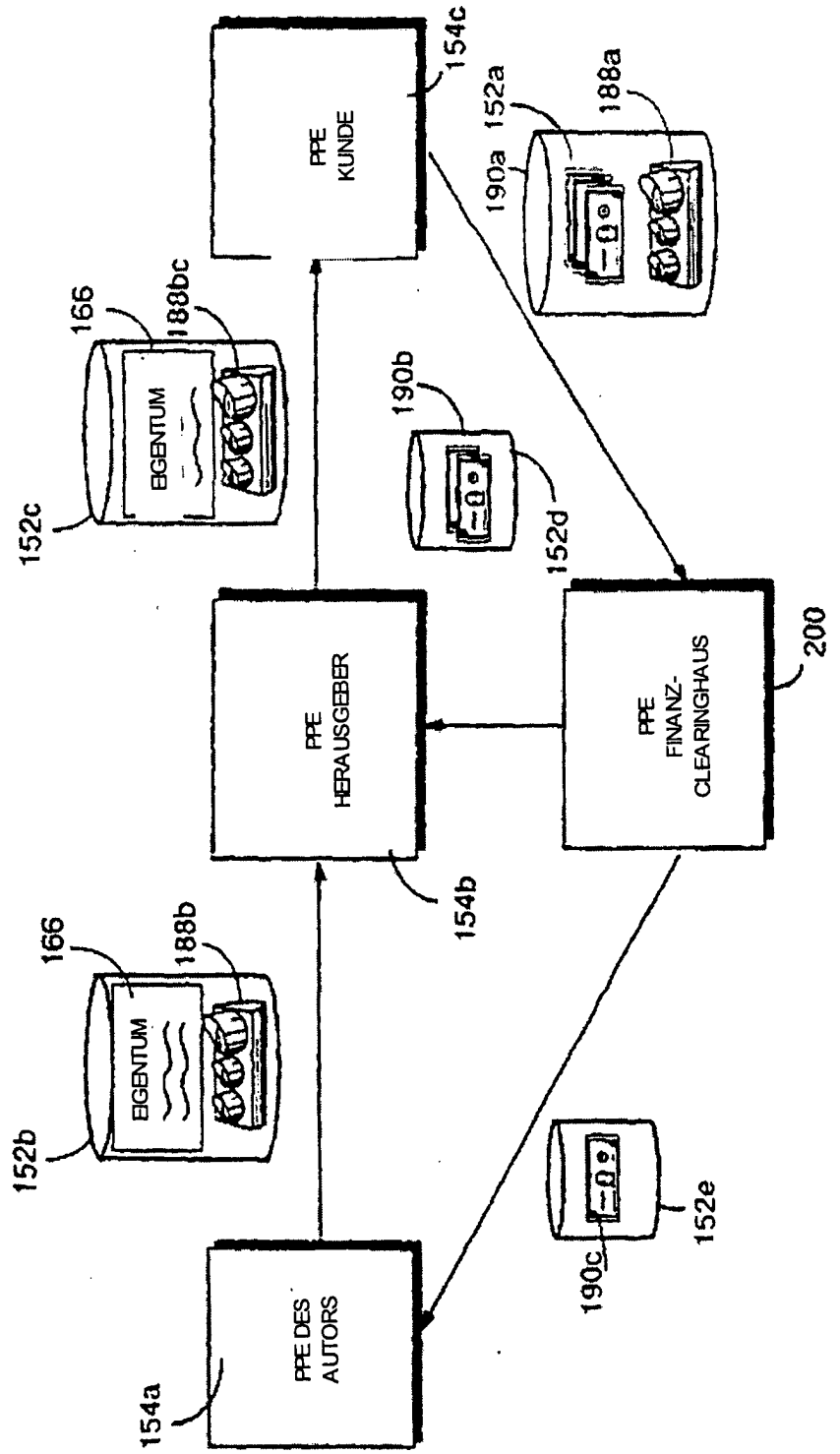


FIG. 22 BEISPIEL FÜR BEZAHLUNG UND UMVERTEILUNG

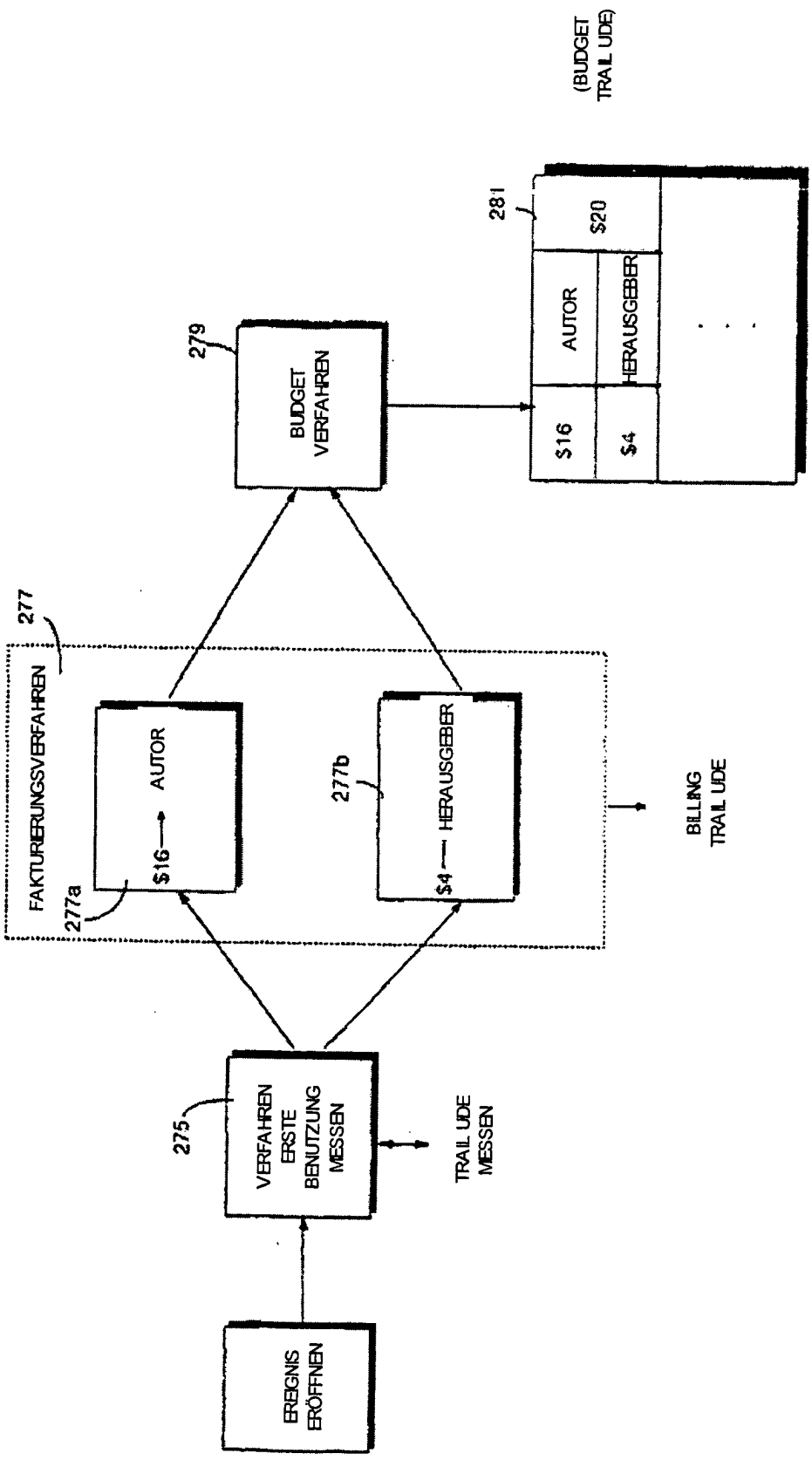


FIG. 22A BEISPIEL FÜR DIE DISAGGREGATION EINES BENUTZERKNOTENS

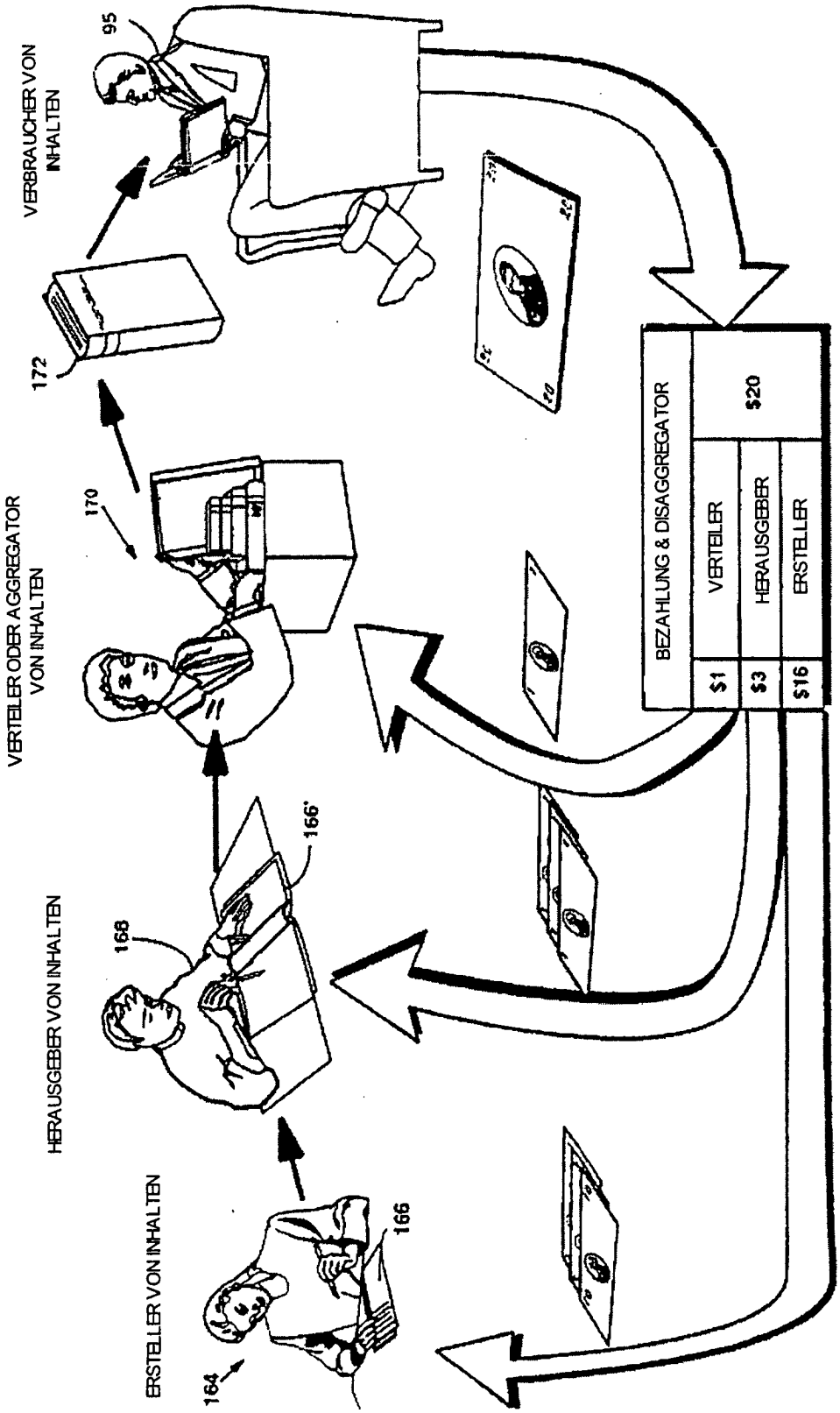


FIG. 23 DISAGGREGATION DER BEZAHLUNG

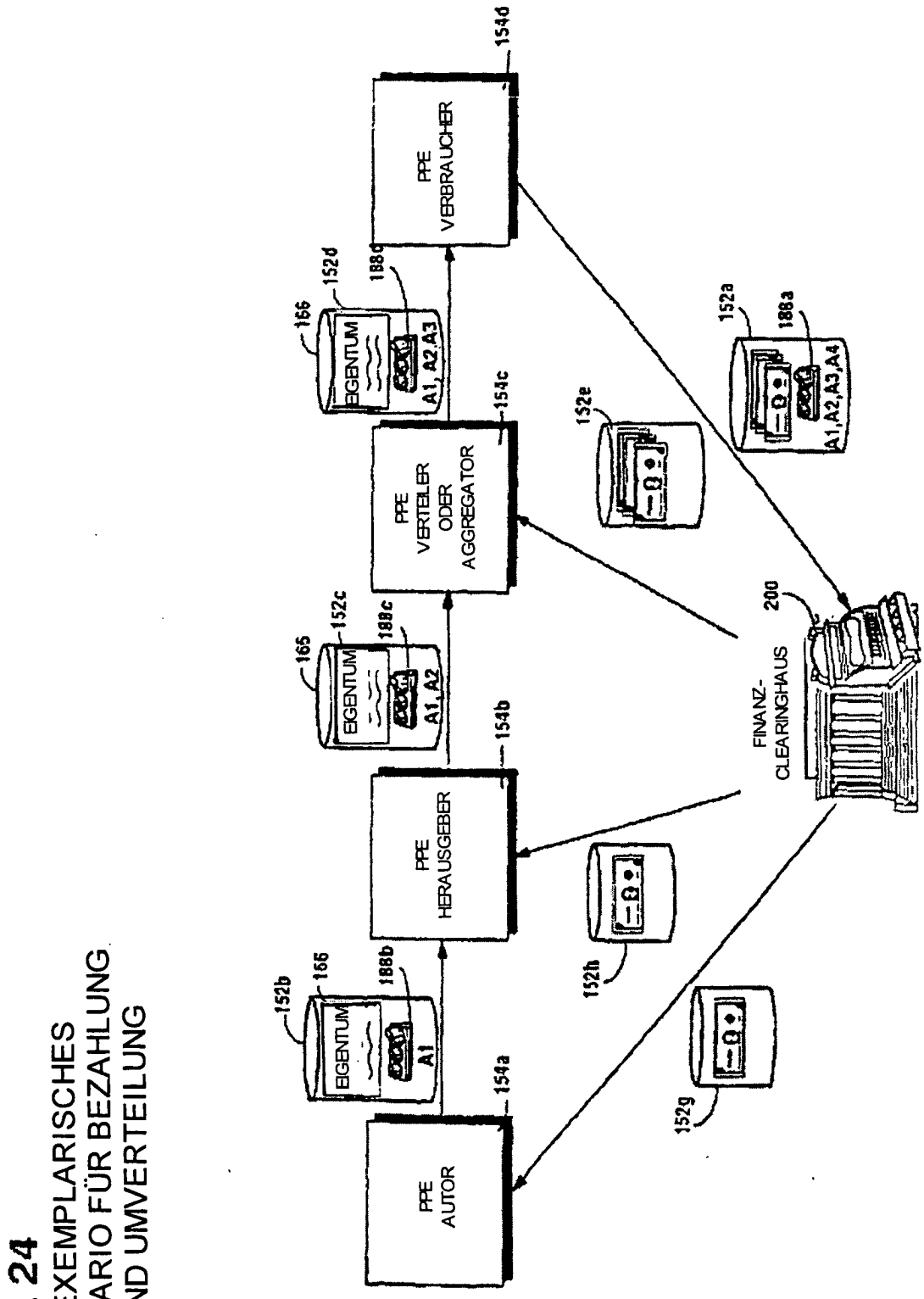


FIG. 24
EXEMPLARISCHES SZENARIO FÜR BEZAHLUNG UND UMVERTEILUNG

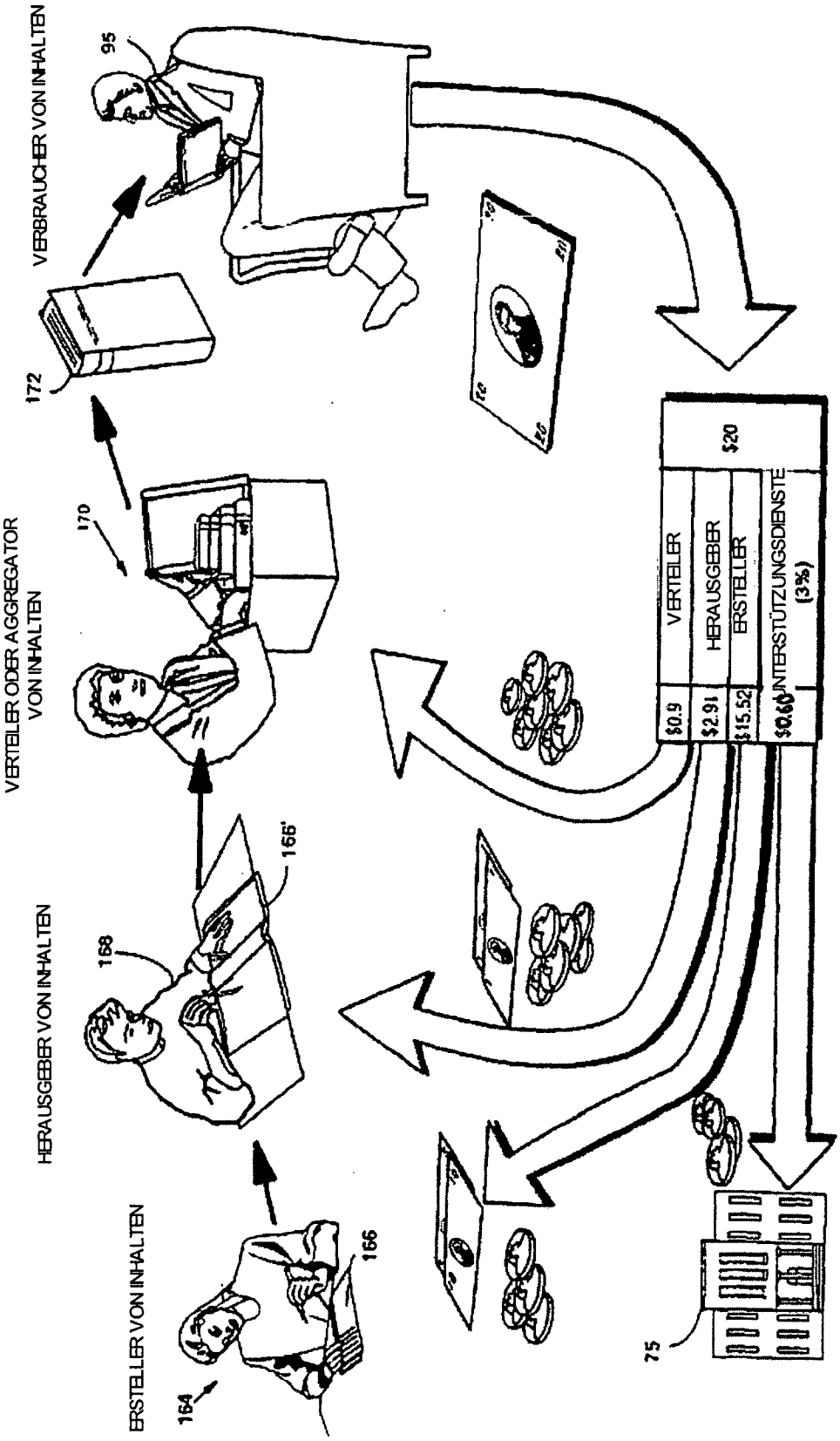


FIG. 25
BEISPIEL FÜR
BEZAHLUNGS-DISAGGREGATION

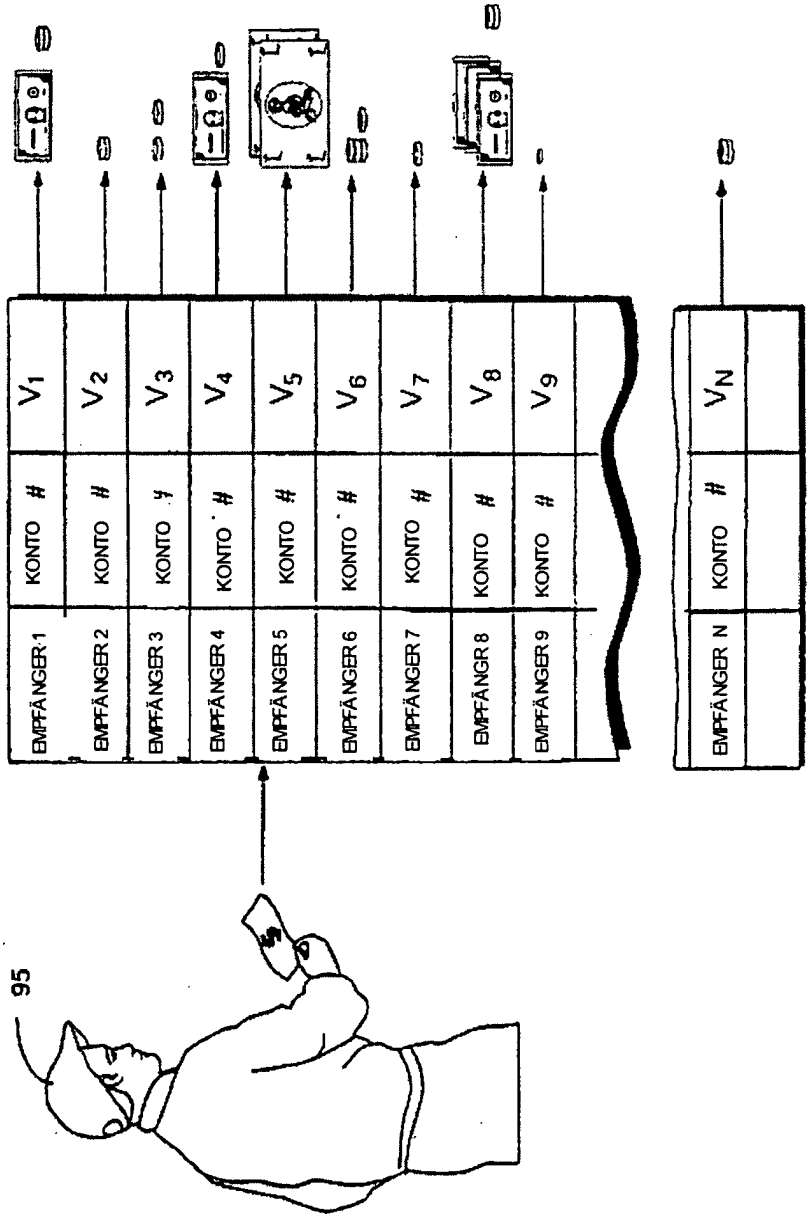


FIG. 26 BEZAHLUNGS-DISAGGREGATION

FIG. 27

Exemplarisches Szenario für Bezahlung und Umverteilung

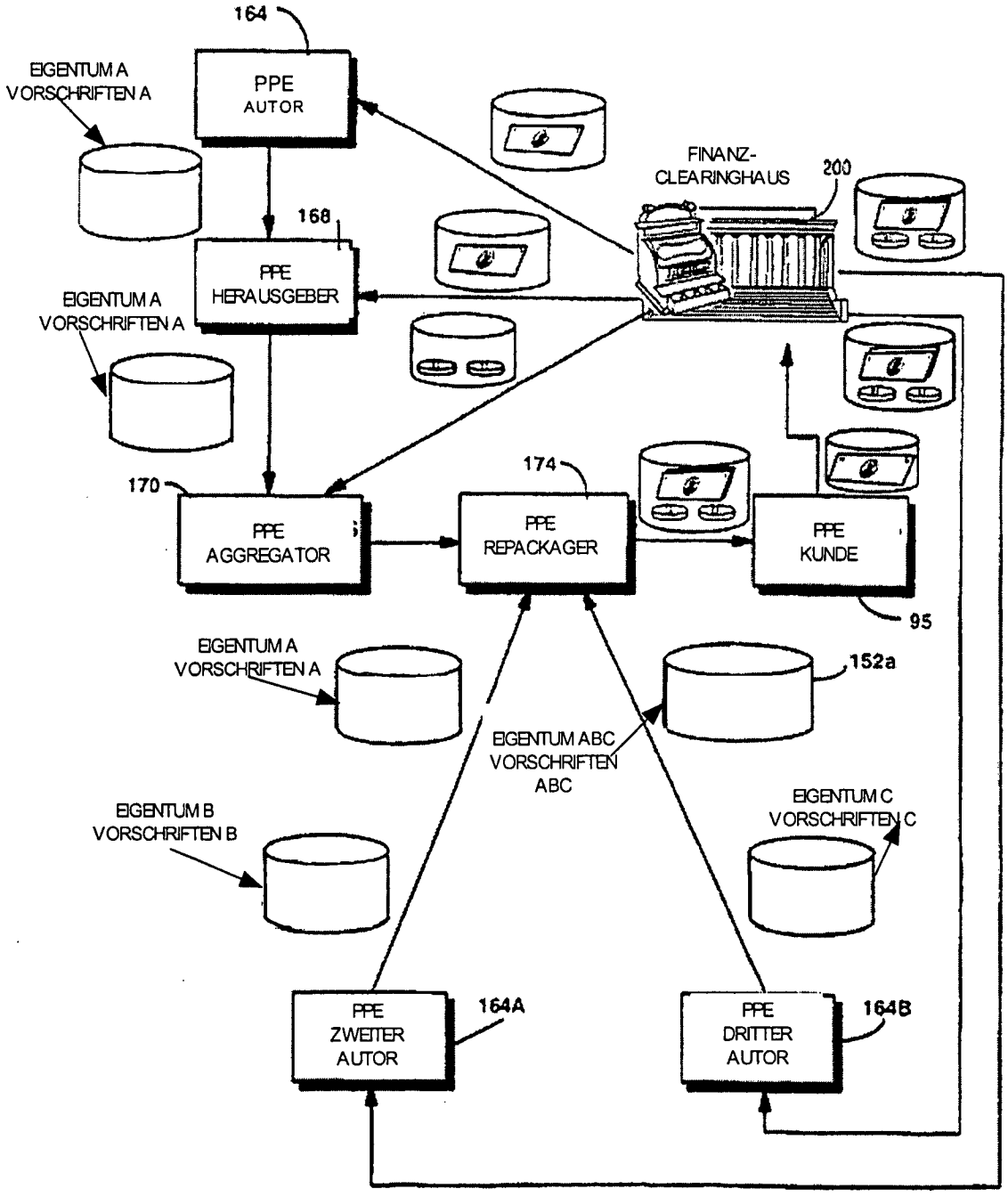
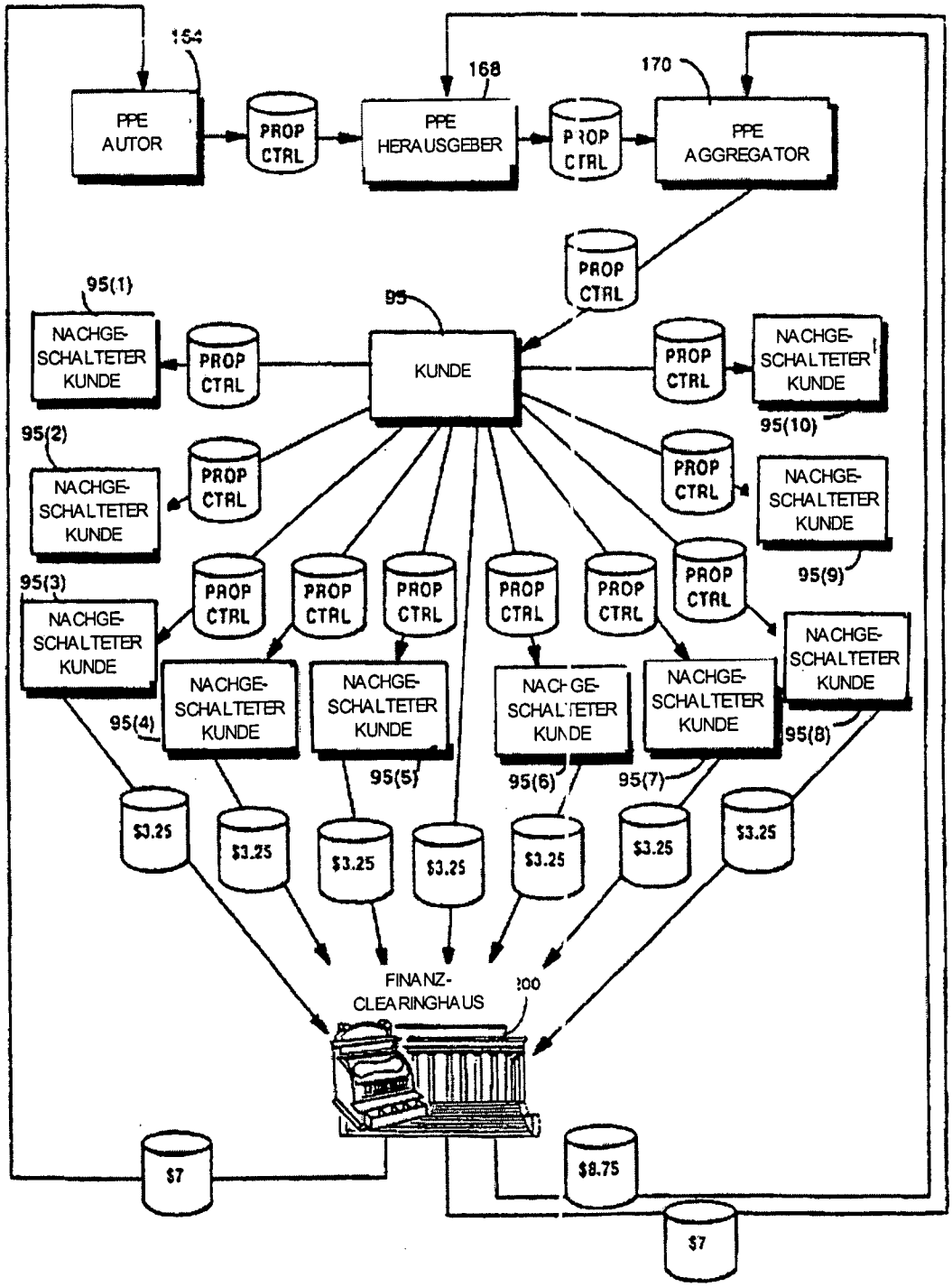


FIG. 28 Beisp el für Superdistribution



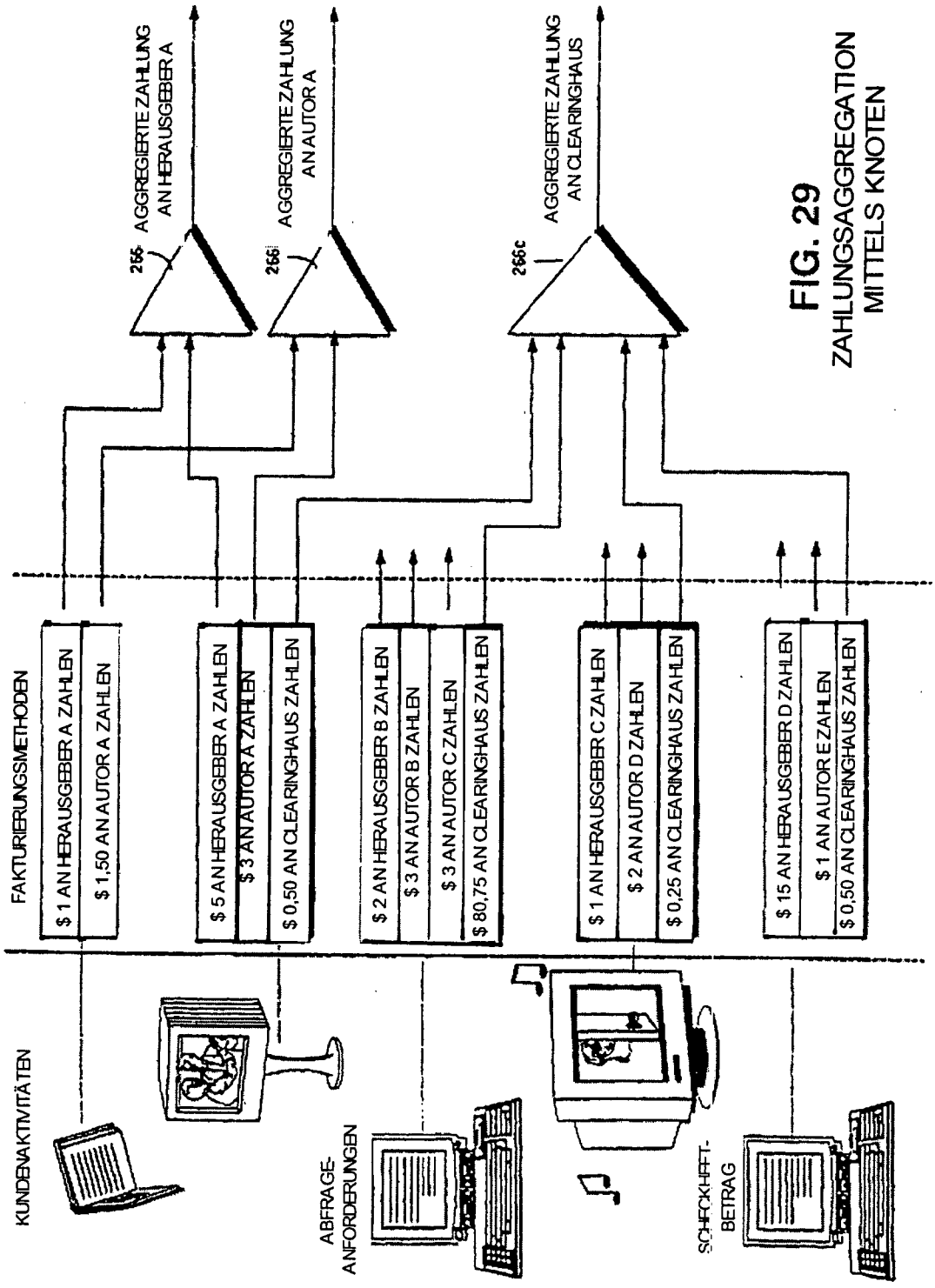


FIG. 29
ZAHLUNGSAGGREGATION MITTELS KNOTEN

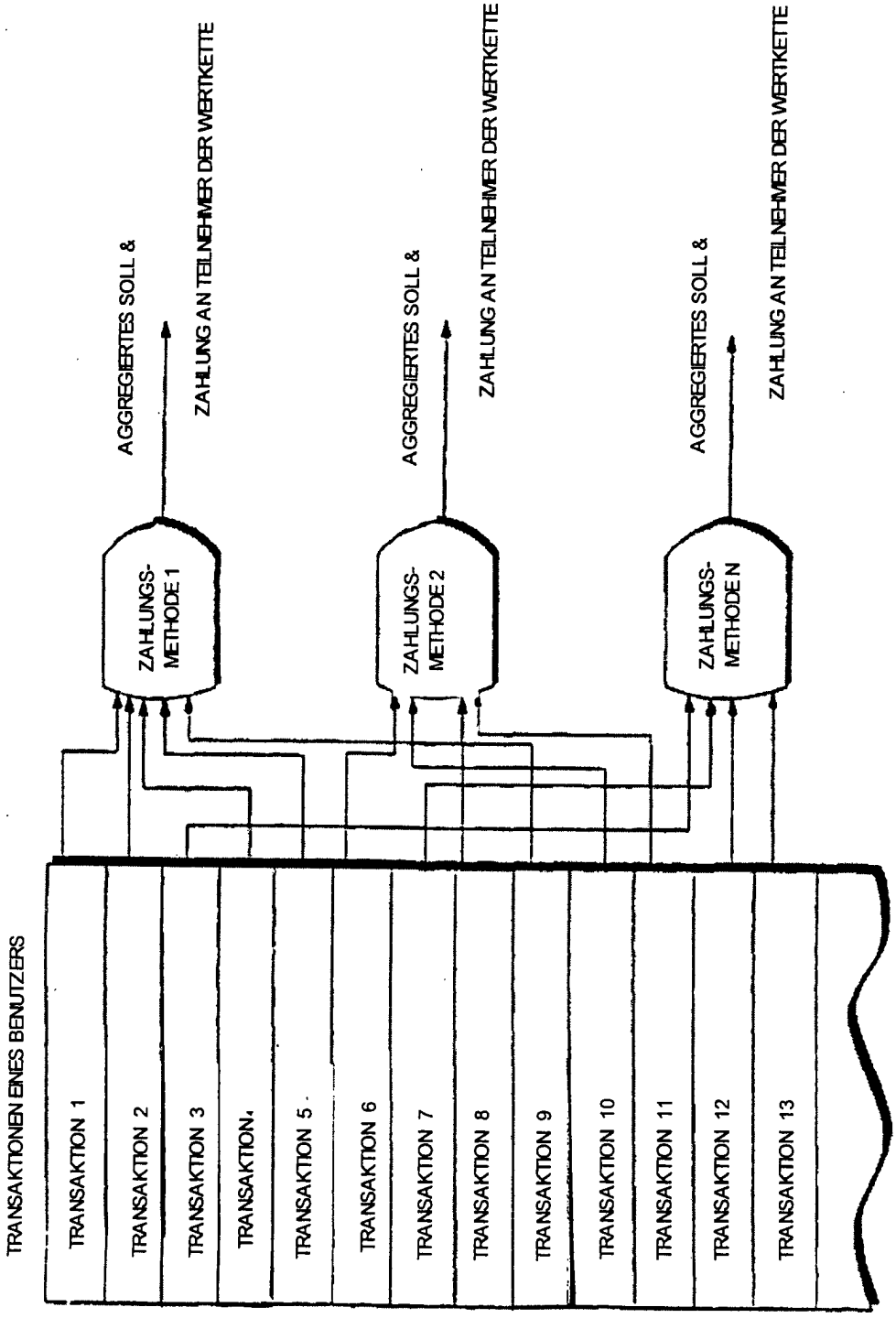


FIG. 30

BEISPIEL FÜR ZAHLUNGSAGGREGATION

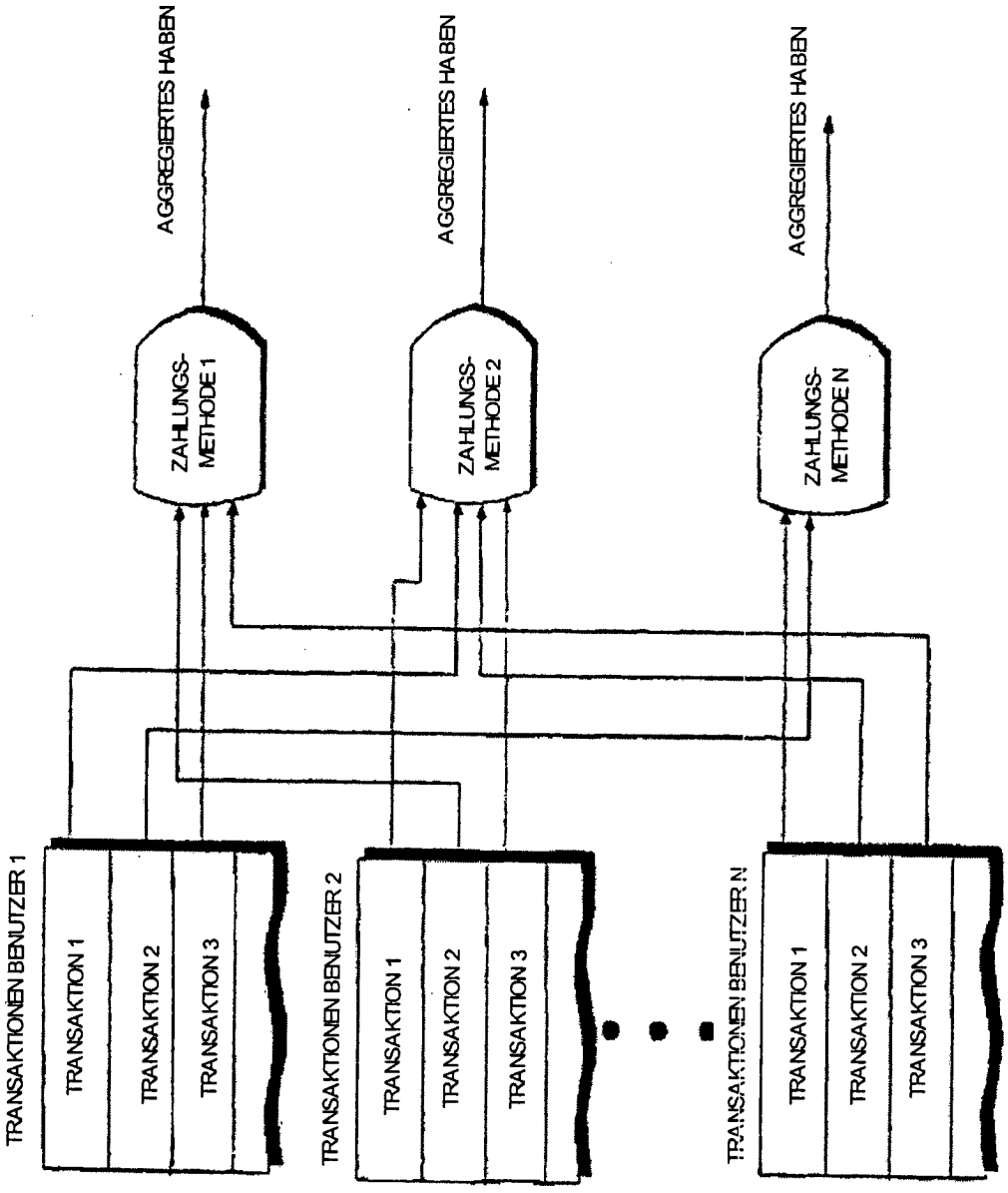
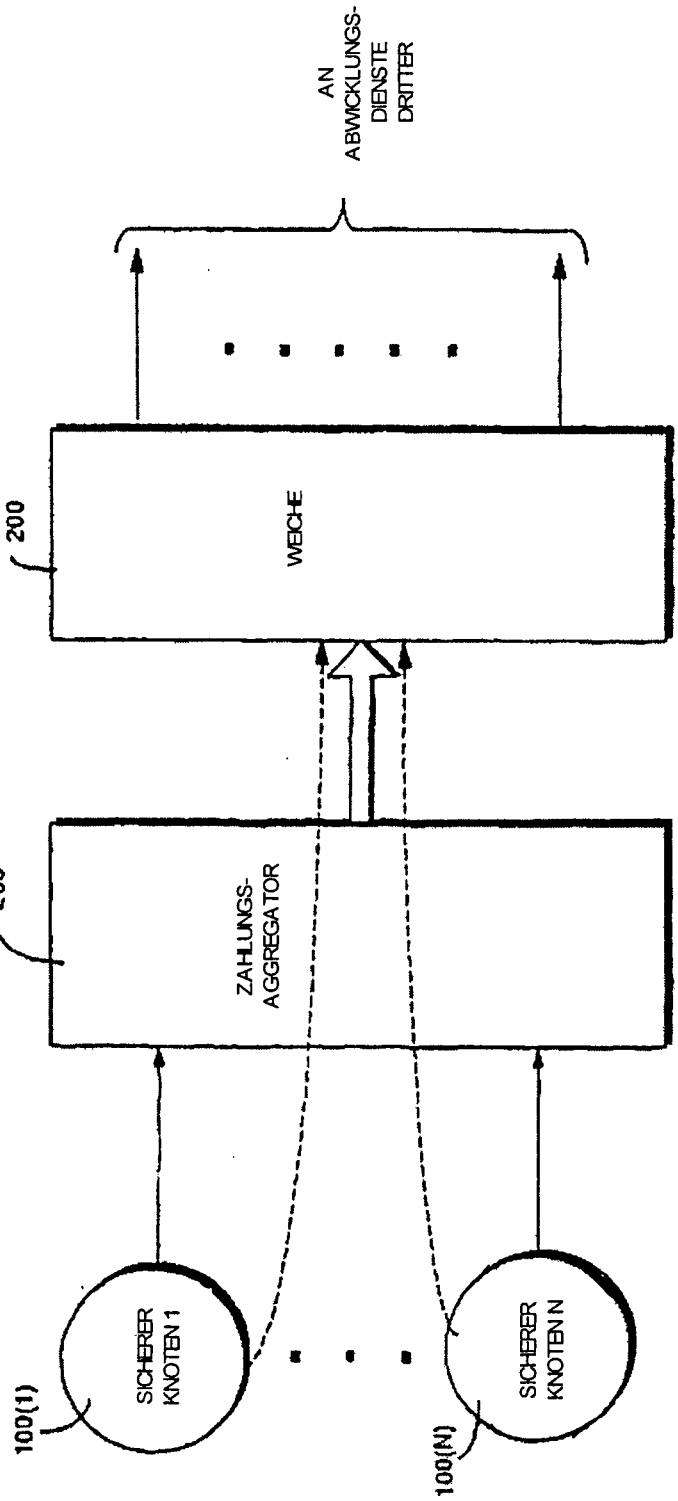


FIG. 31 BEISPIEL FÜR ZAHLUNGSAGGREGATION BEIM FINANZ-CLEARINGHAUS

FIG. 32 EXEMPLARISCHE ANORDNUNG EINES FINANZ-CLEARINGHAUSES



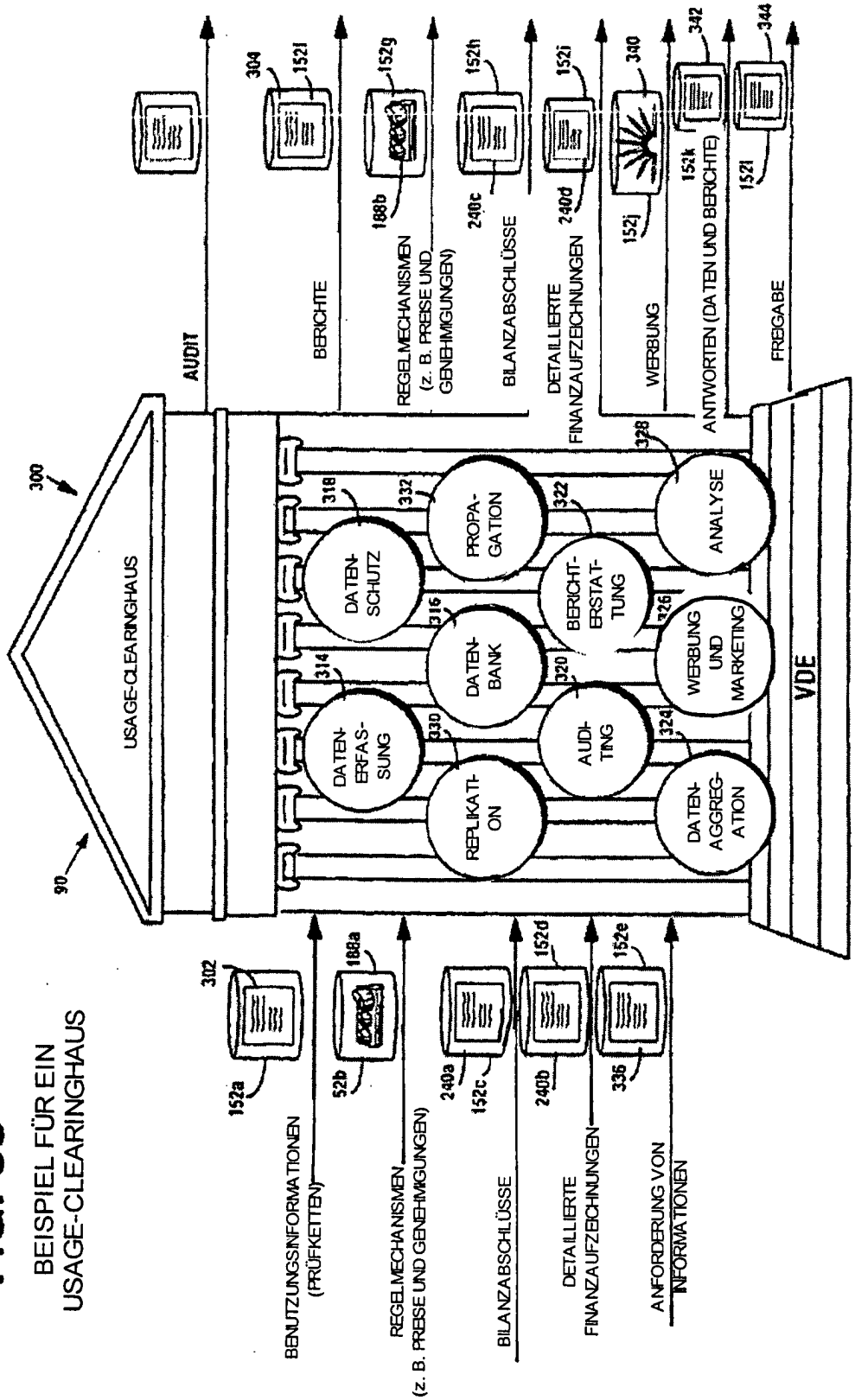


FIG. 33

BEISPIEL FÜR EIN USAGE-CLEARINGHAUS

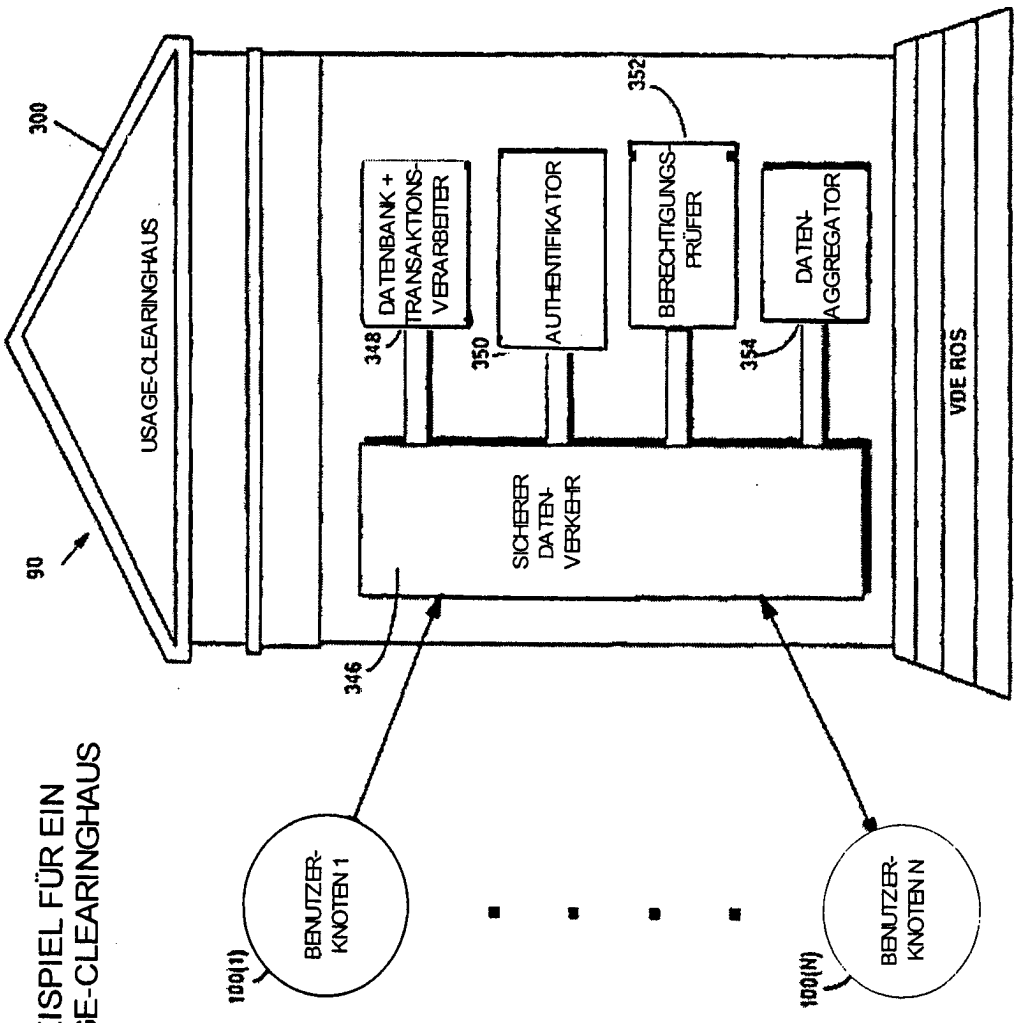


FIG. 34

BEISPIEL FÜR EIN USAGE-CLEARINGHAUS

FIG. 35 EXEMPLARISCHER ABLAUF BEIM USAGE-CLEARING

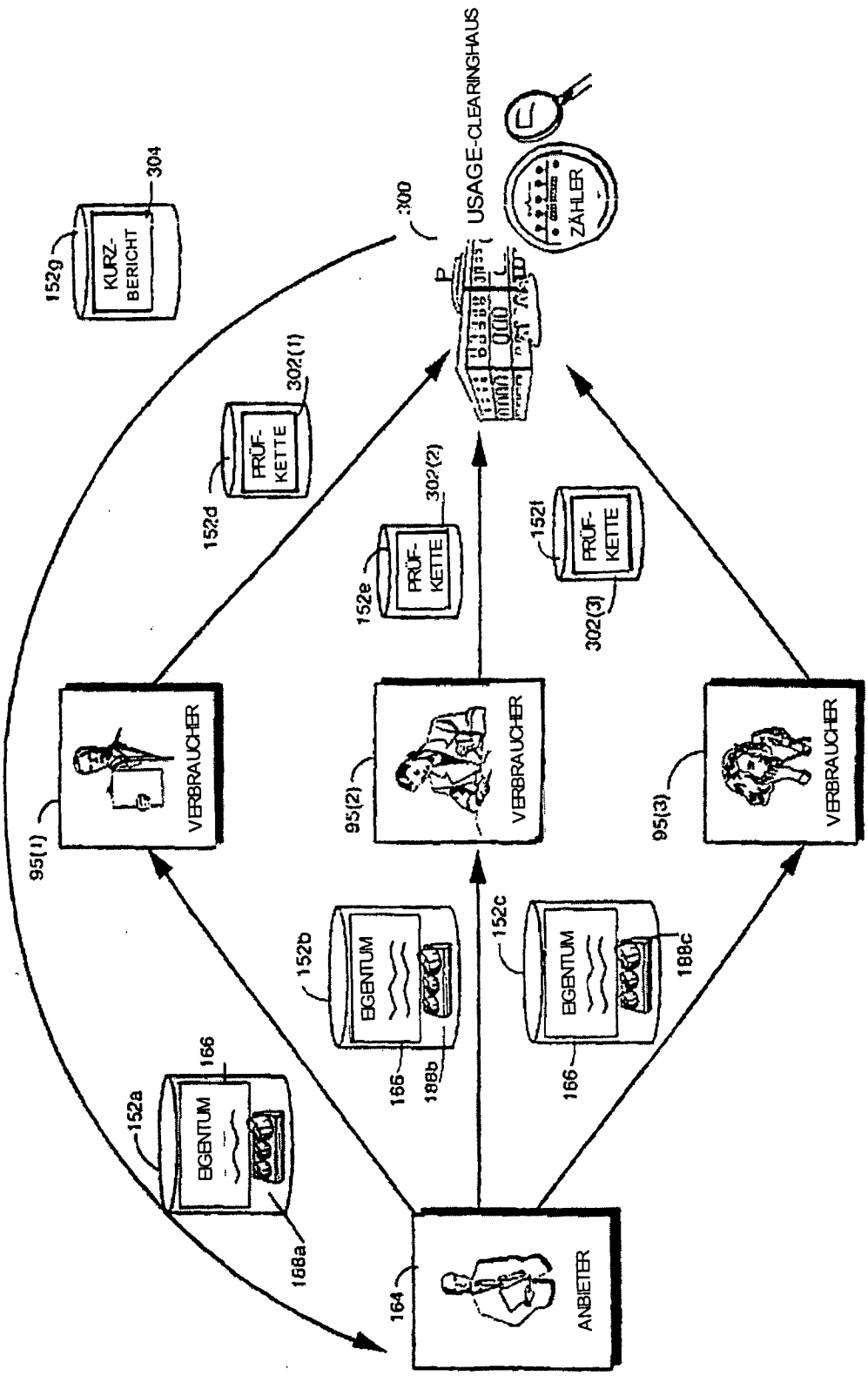


FIG. 36 EXEMPLARISCHER ABLAUF BEIM USAGE-CLEARING

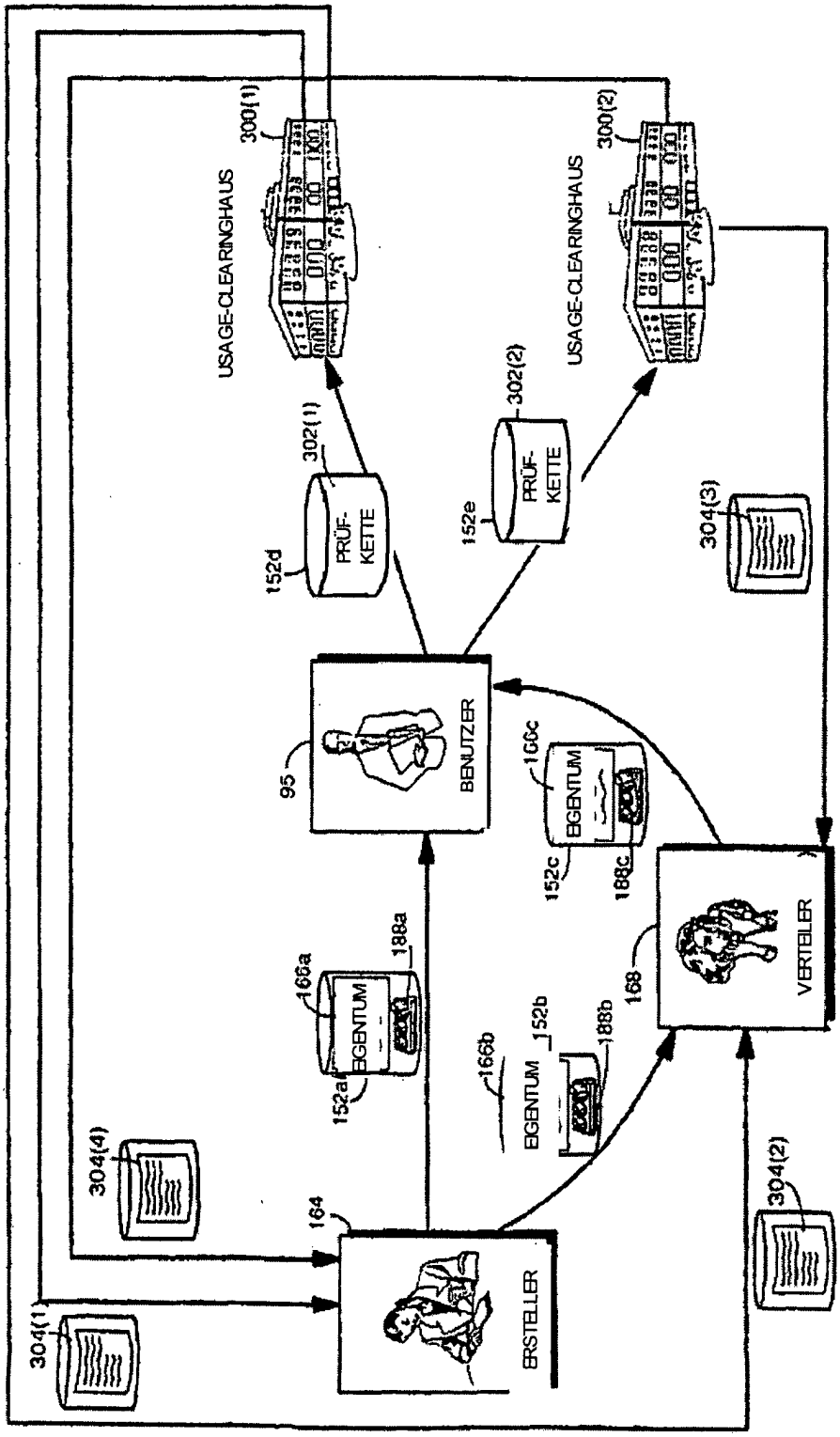


FIG. 37 EXEMPLARISCHER ABLAUF IM FINANZ- UND USAGE-CLEARINGHAUS

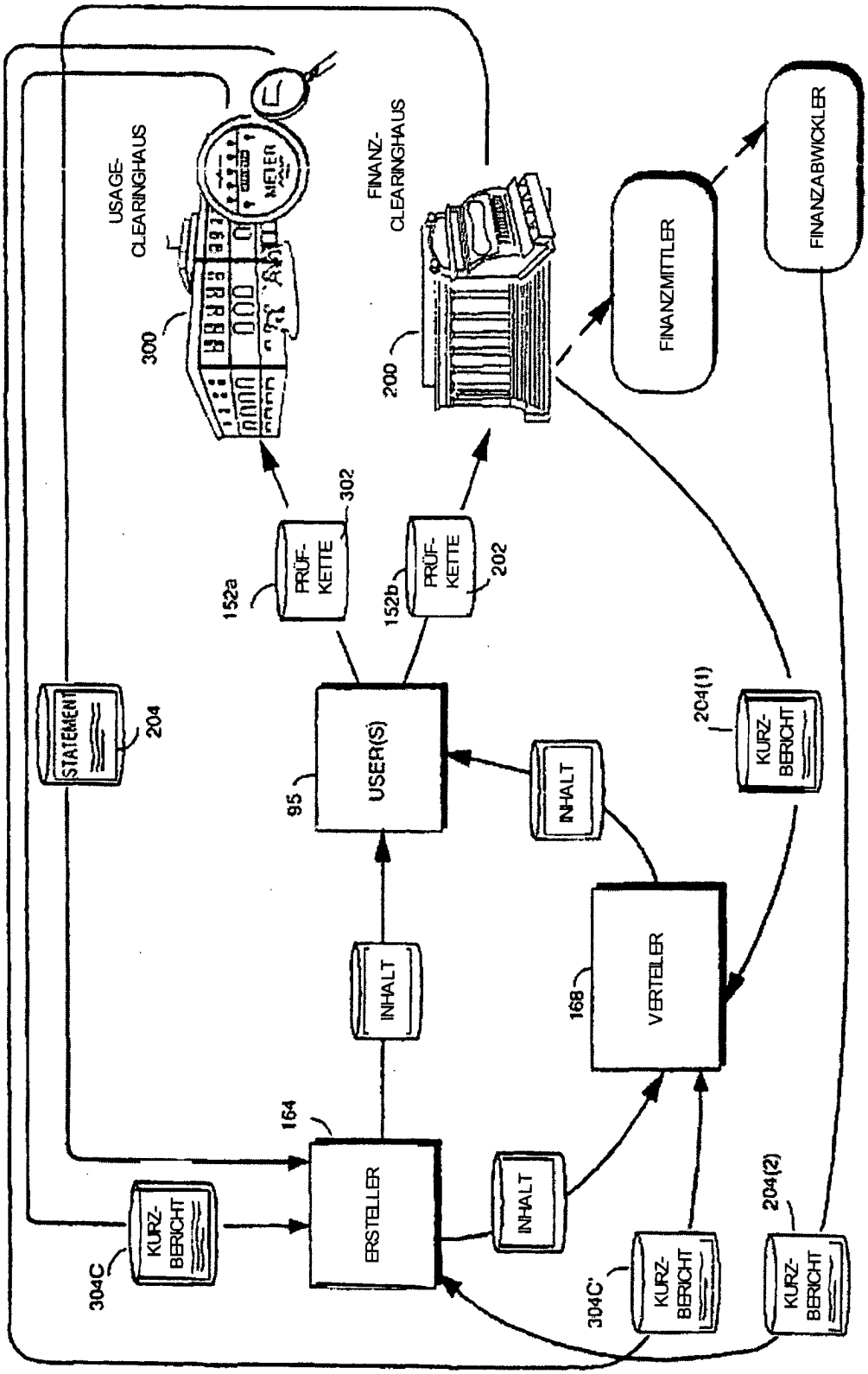


FIG. 38 BEISPIEL FÜR MEDIENPLATZIERUNG IM USAGE-CLEARINGHAUS

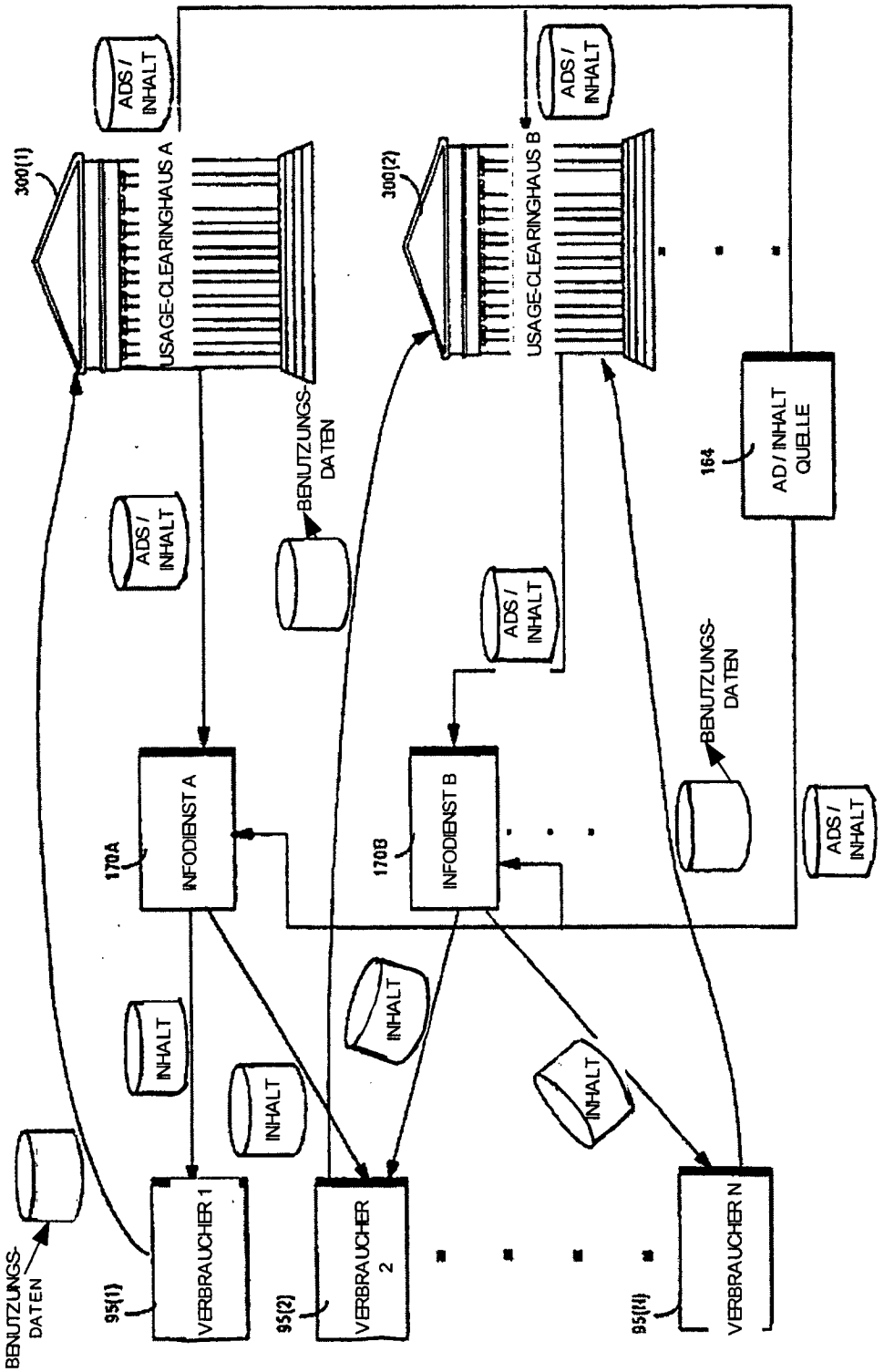
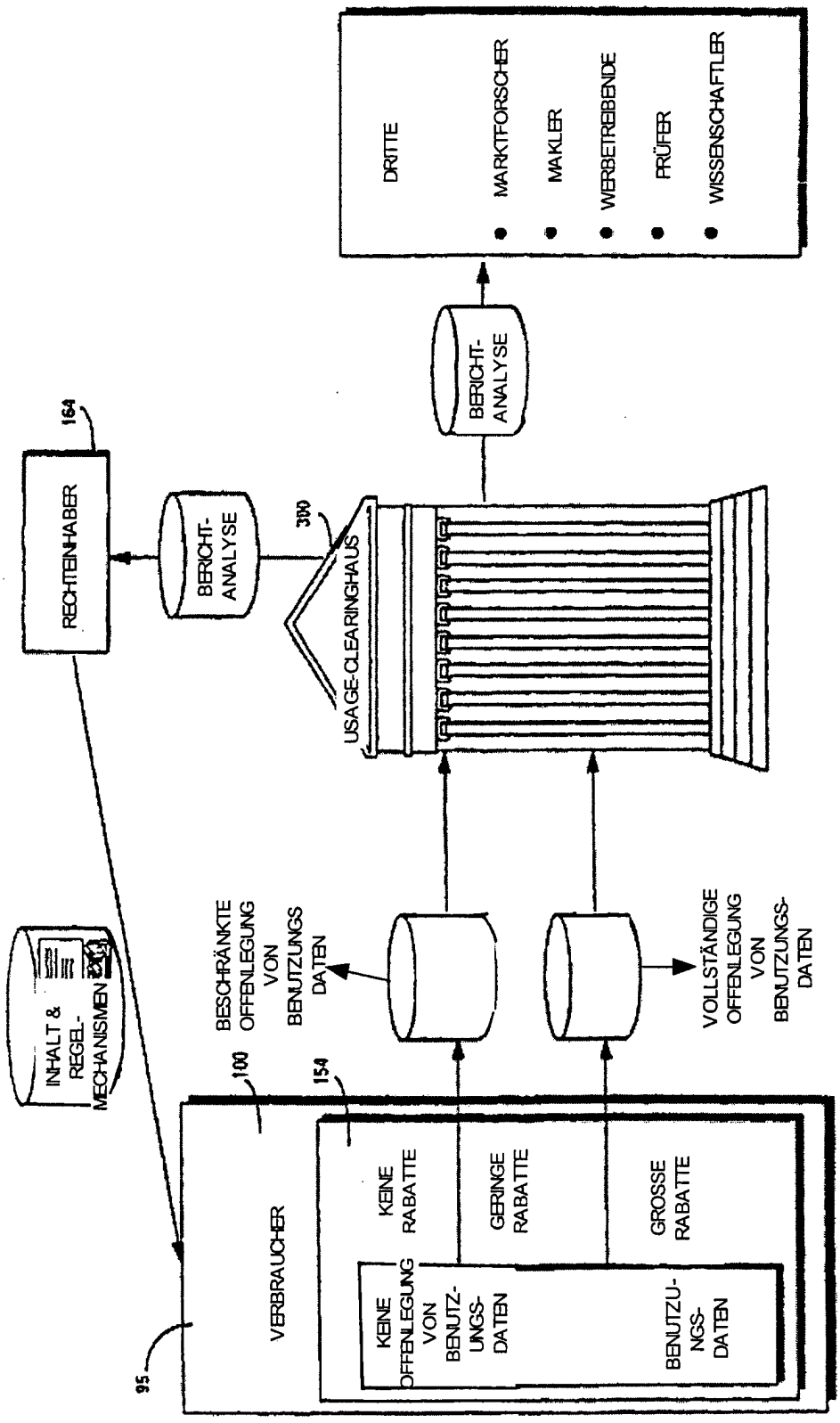


FIG. 39
BEISPIEL FÜR EIN CLEARINGHAUS
RABATTE AUF GRUNDLAGE VON OFFENLEGUNG



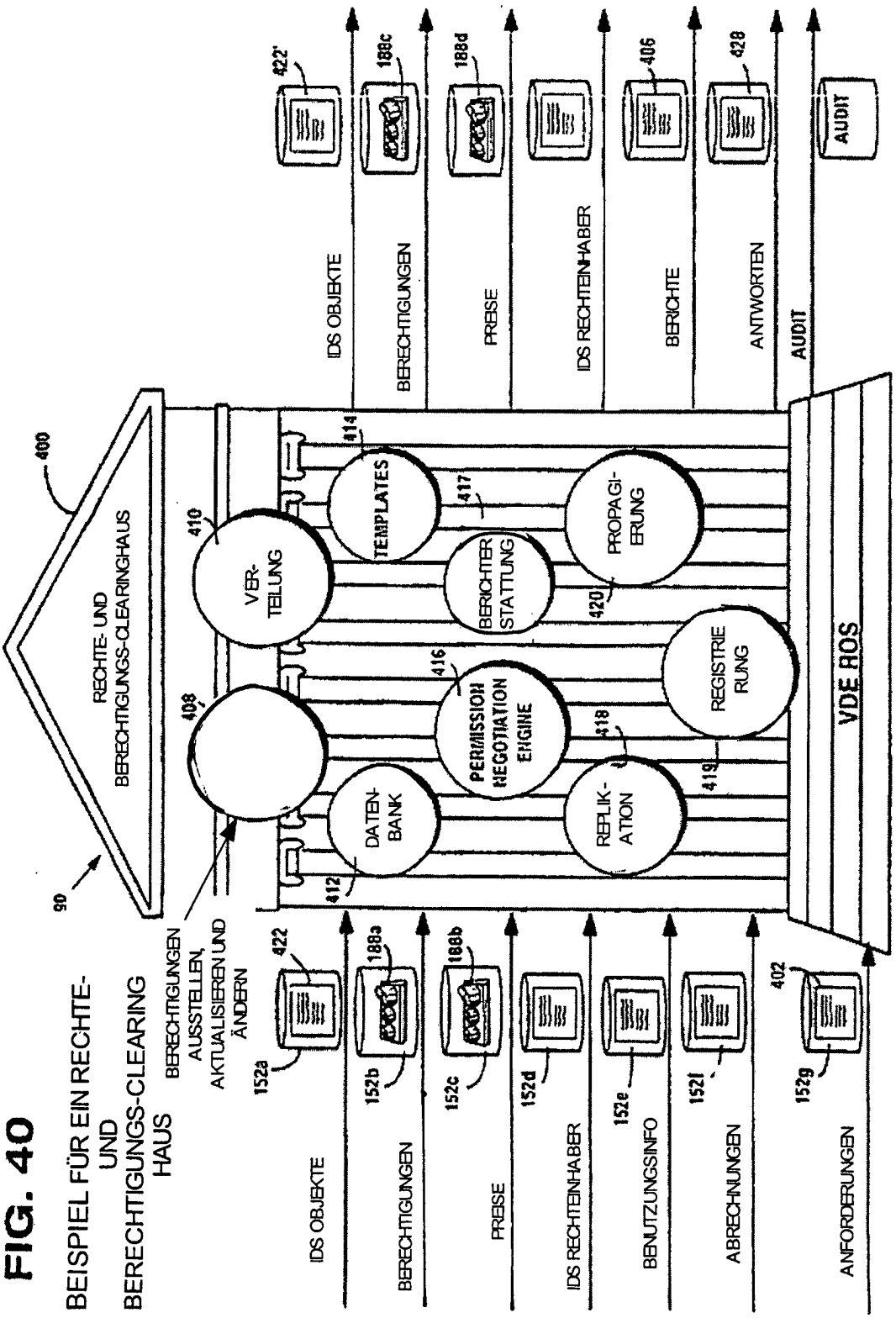


FIG. 40

BEISPIEL FÜR EIN RECHTE- UND BERECHTIGUNGS-CLEARING HAUS

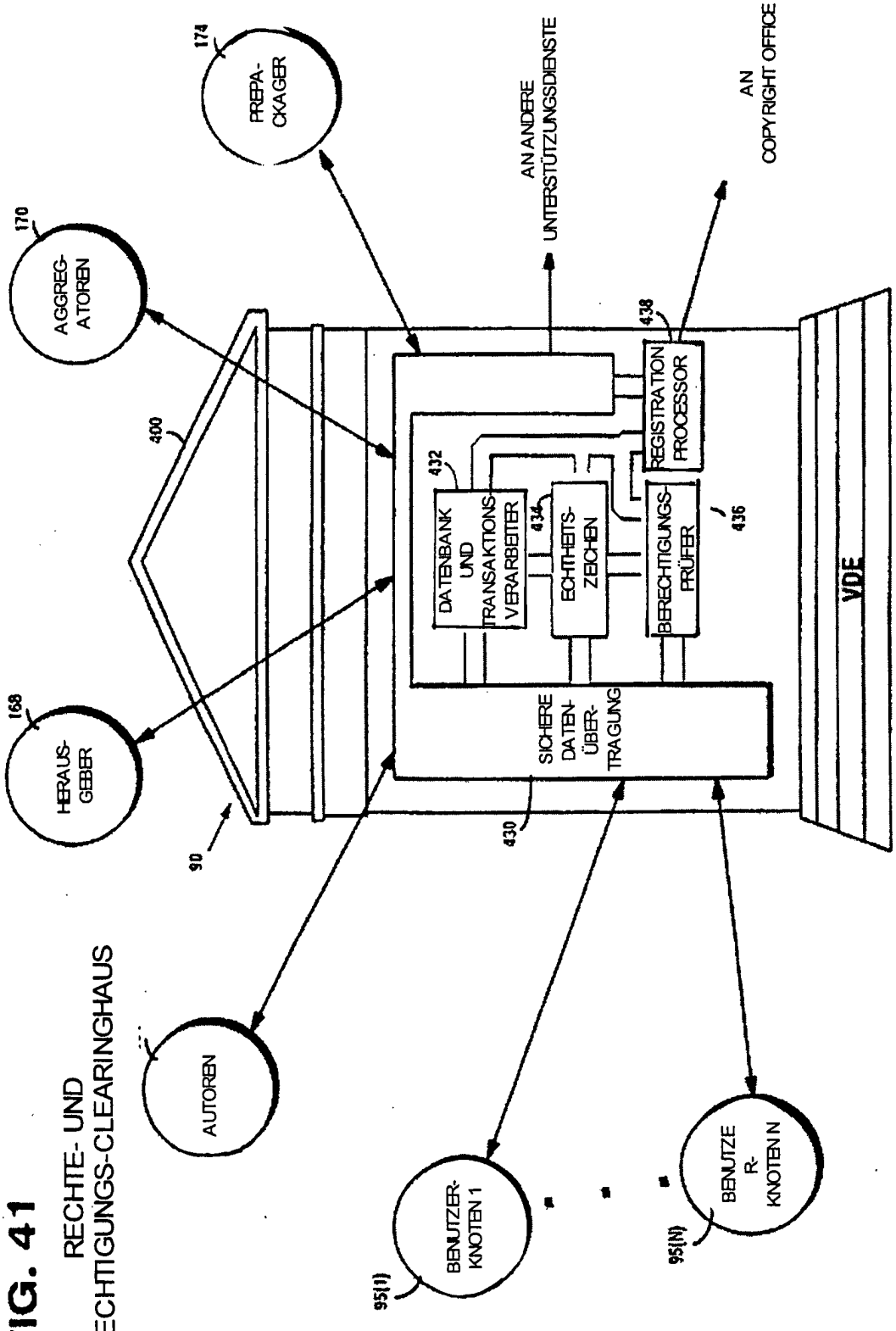
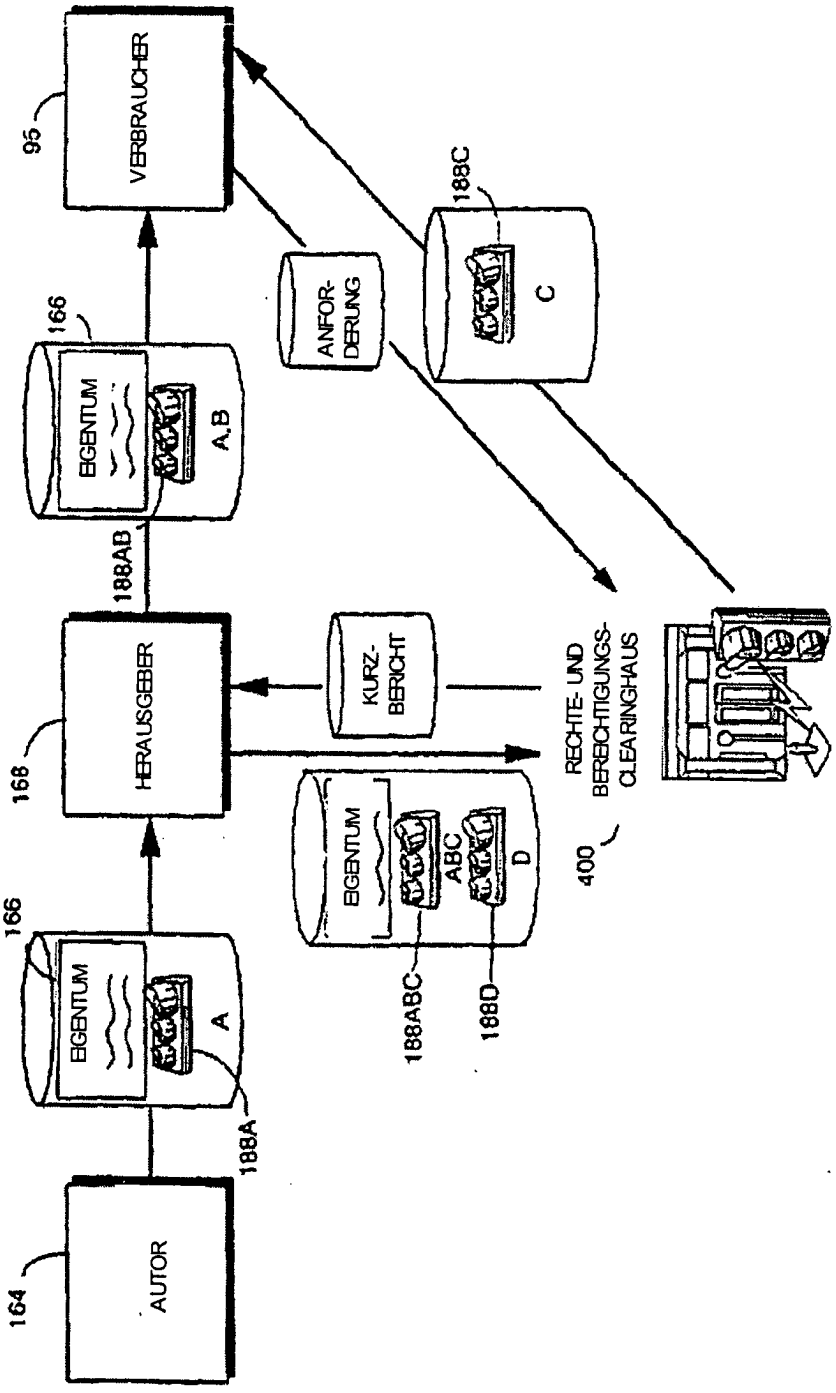


FIG. 41
RECHTE- UND BERECHTIGUNGS-CLEARINGHAUS

FIG. 42

BEISPIEL DES ABLAUFS IN EINEM RECHTE- UND BERECHTIGUNGS-CLEARINGHAUS



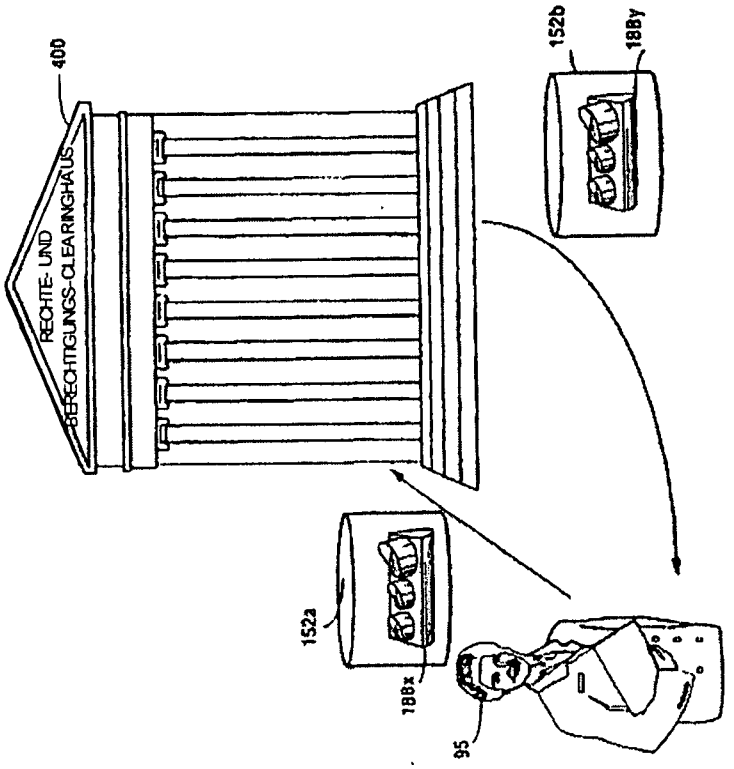
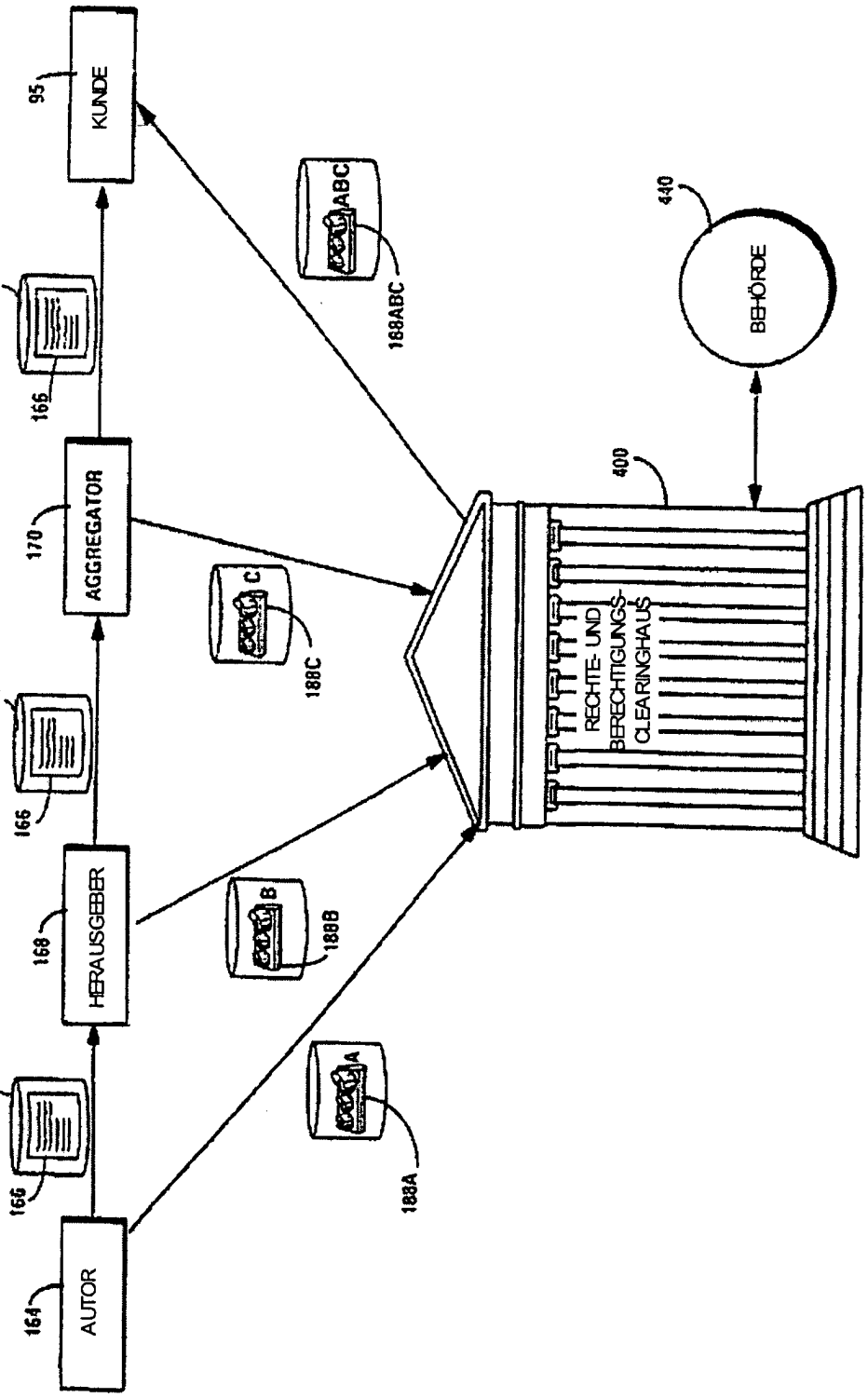
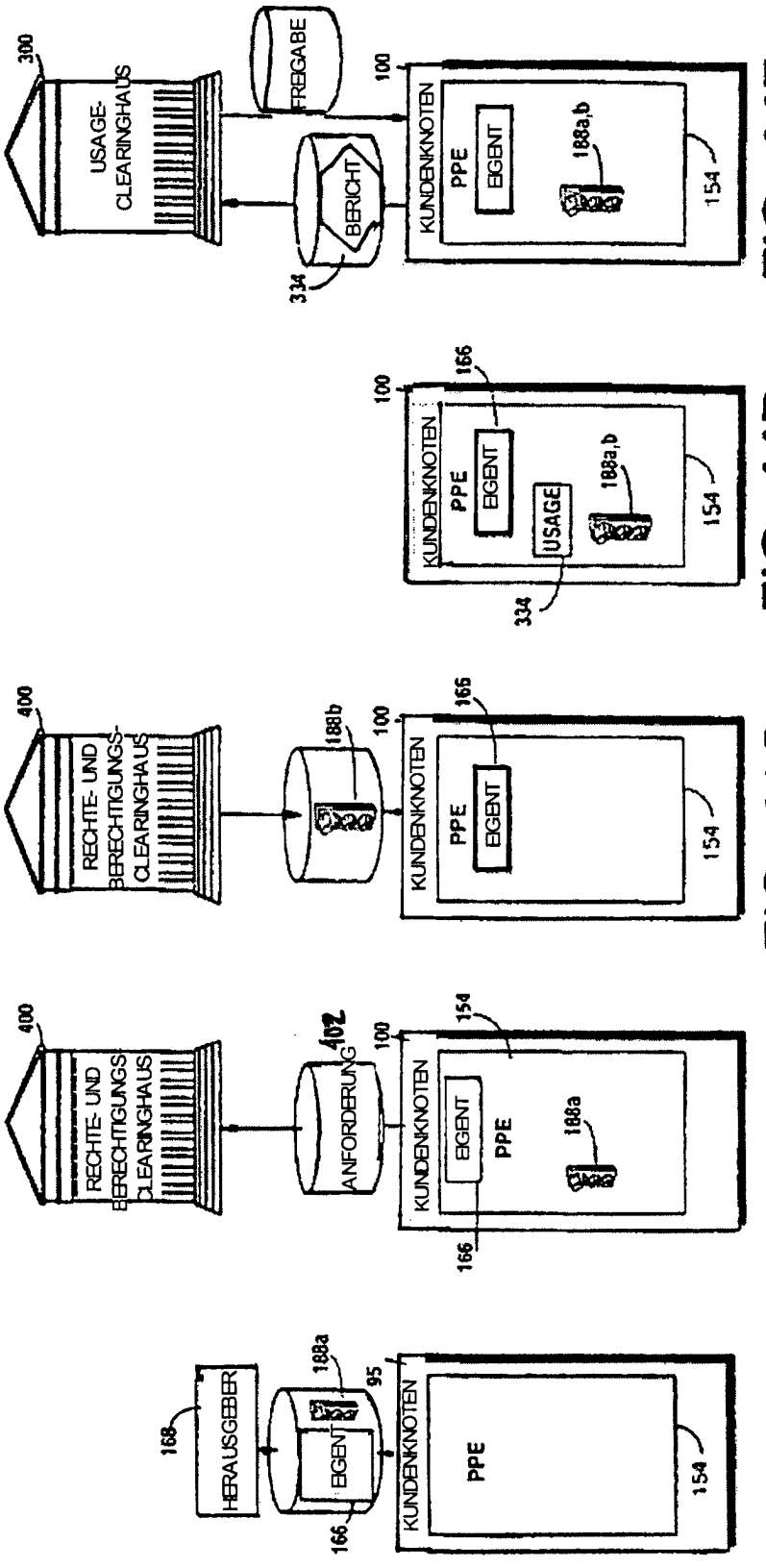


FIG. 42A

VERBRAUCHER REGISTRIERT REGELSATZ, UM UPDATES ANZUFORDERN

FIG. 43 BEISPIEL FÜR EINE RECHTE- UND BERECHTIGUNGS-WERTKETTE




HERAUSGEBER
168
EIGENT
188a
95
166
KUNDENKNOTEN
PPE
154
FIG. 44A
KUNDE ERHÄLT EIGENTUM
RECHTE- UND BERECHTIGUNGS-CLEARINGHAUS
400
ANFORDERUNG
402
188a
EIGENT
166
KUNDENKNOTEN
PPE
154
100
FIG. 44B
KUNDE FORDERT NUTZUNGSRECHTE FÜR DAS EIGENTUM AN
RECHTE- UND BERECHTIGUNGS-CLEARINGHAUS
400
188b
KUNDENKNOTEN
PPE
EIGENT
166
154
100
FIG. 44C
RECHTE- UND BERECHTIGUNGS-C LEARINGHAUS STELLT RECHTE FÜR DEN KUNDEN BEREIT
KUNDENKNOTEN
PPE
EIGENT
USAGE
188a,b
154
166
334
100
FIG. 44D
KUNDE VERWENDET EIGENTUM GEMÄß DEN ERTEILTEN RECHTEN
USAGE-CLEARINGHAUS
300
FREIGABE
BERICHT
334
KUNDENKNOTEN
PPE
EIGENT
188a,b
154
100
FIG. 44E
KUNDENKNOTEN BERICHTET ÜBER ASPEKTE DER BENUTZUNG

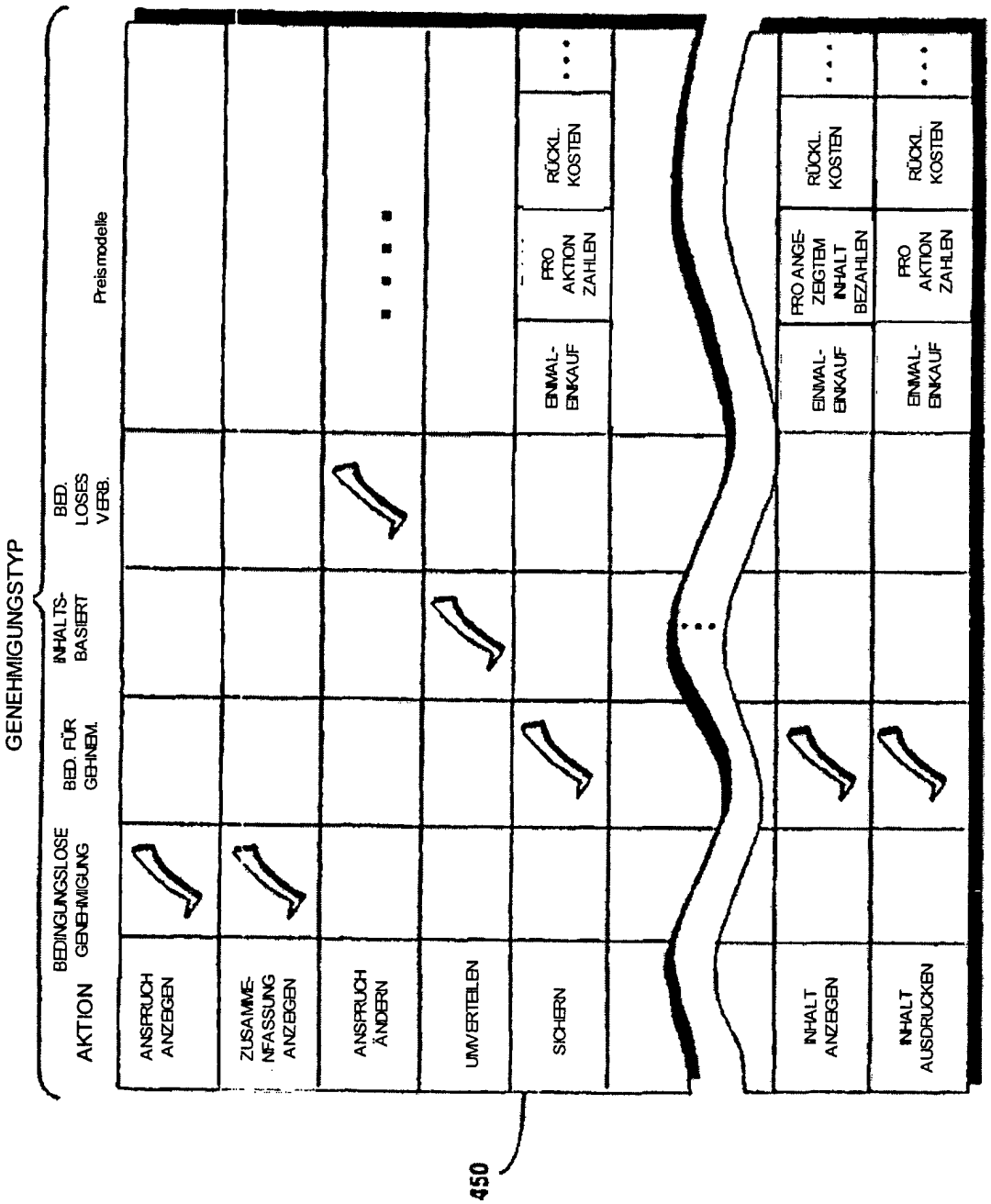


FIG. 45A

BEISPIEL FÜR EIN RECHTETEMPLATE

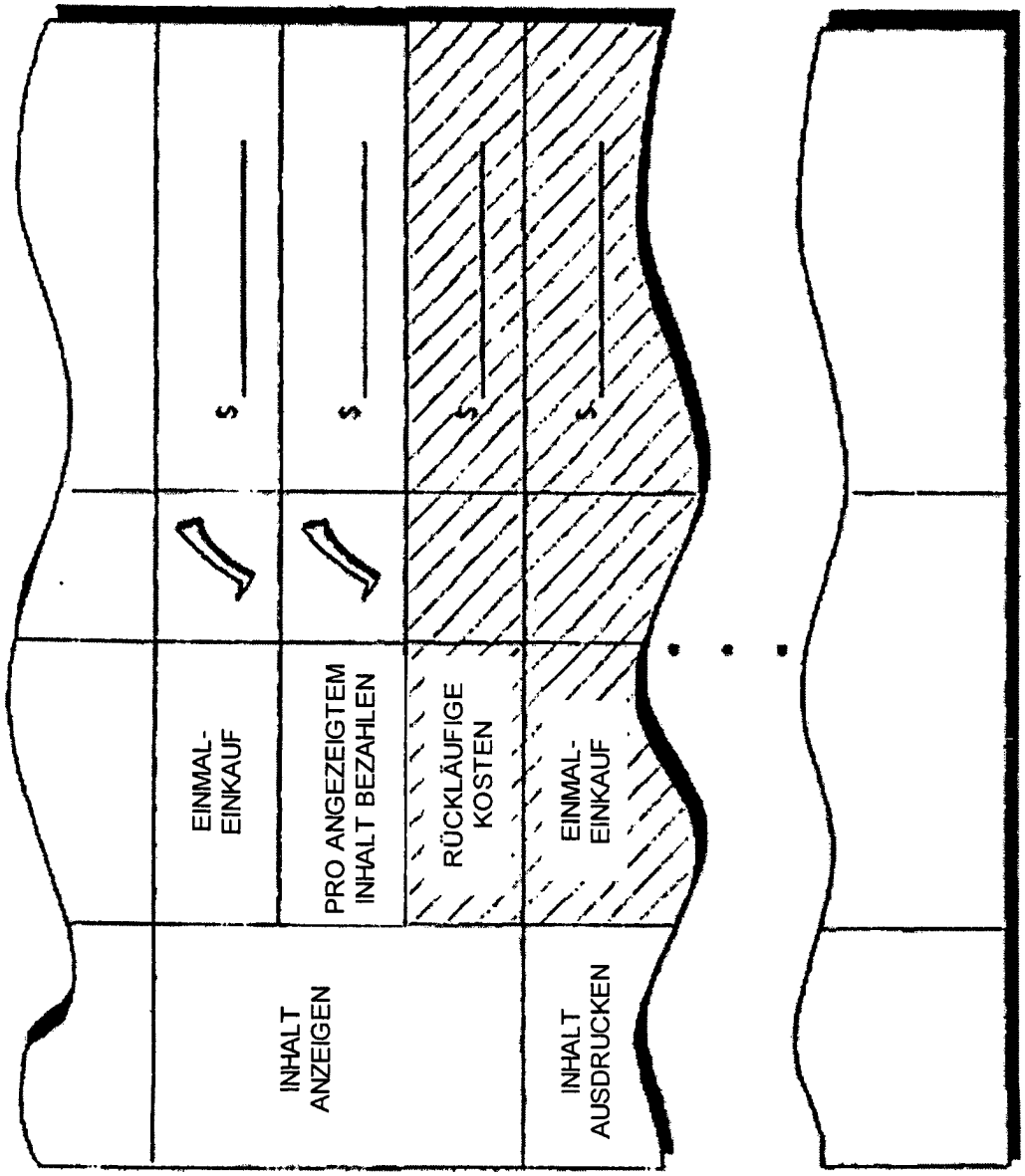


FIG. 45B PREISMODELLE UND -EBENEN

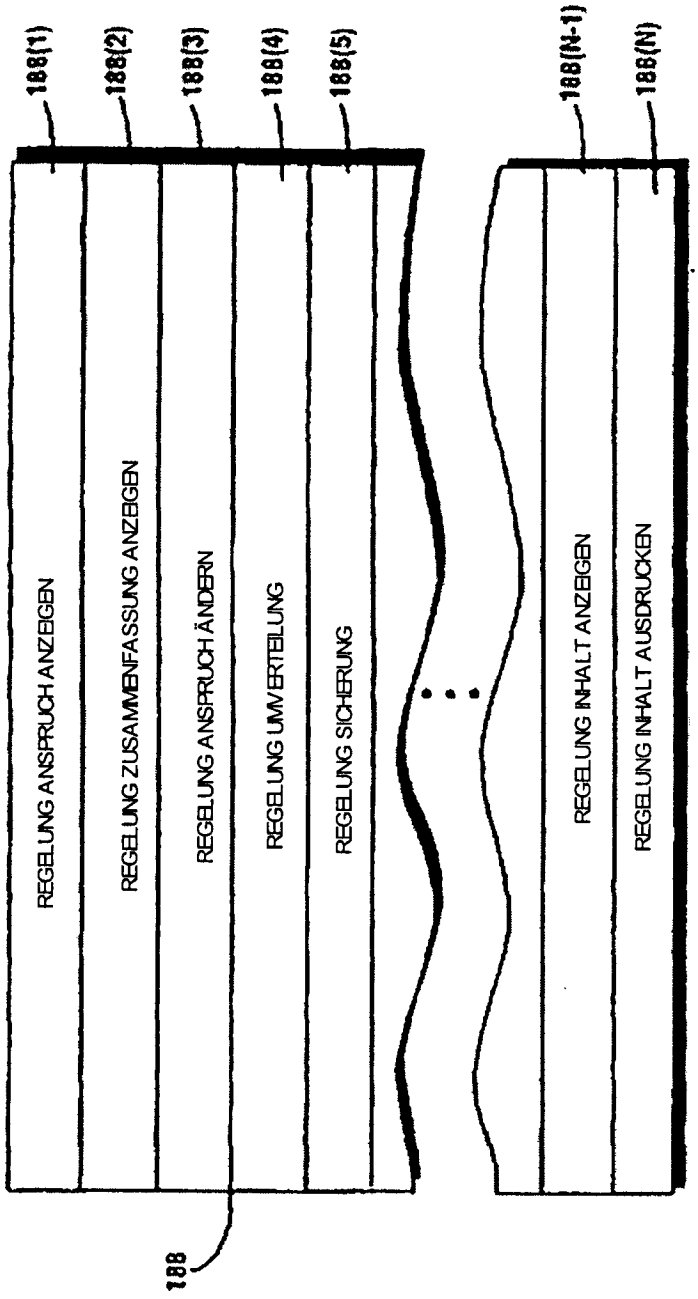
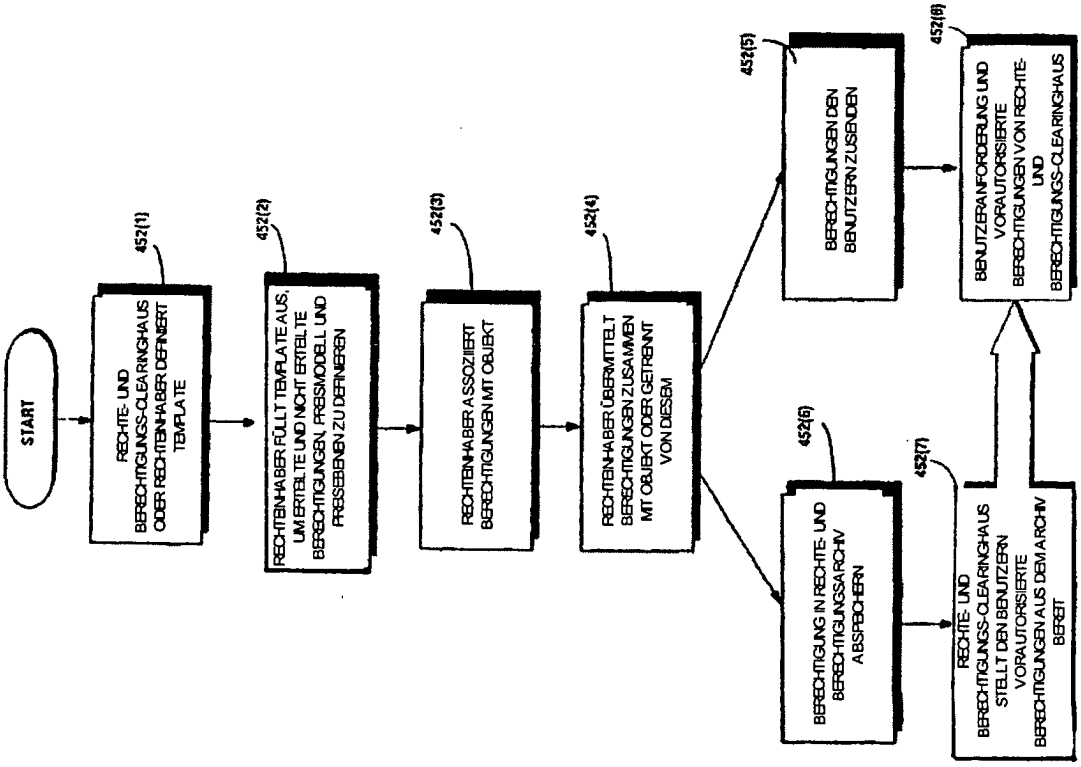


FIG. 45C BEISPIEL FÜR EINEN REGELSATZ

FIG. 46 BEISPIEL FÜR EINEN RECHTE- UND BERECHTIGUNGS-CLEARINGABLAUF



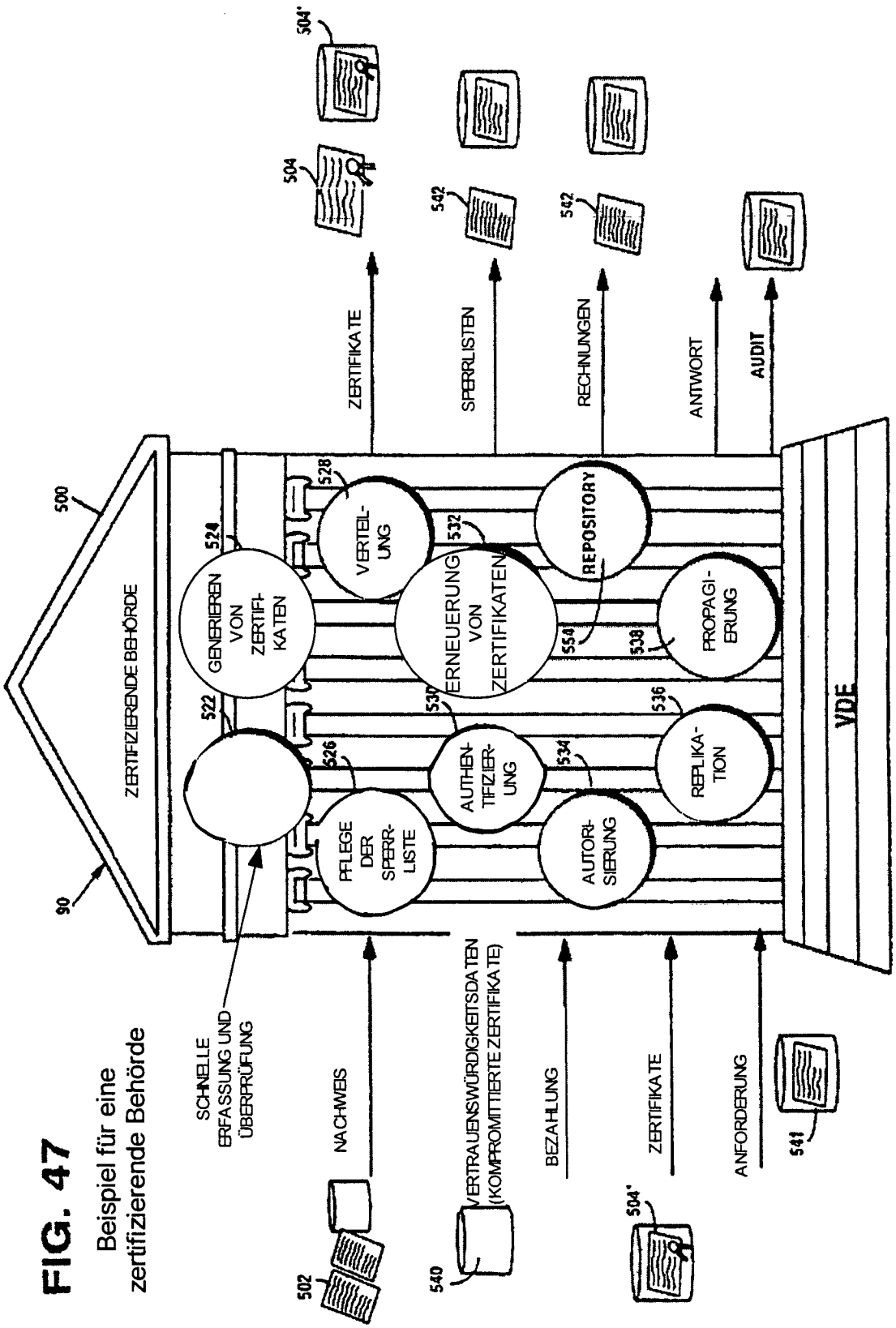


FIG. 47

Beispiel für eine zertifizierende Behörde

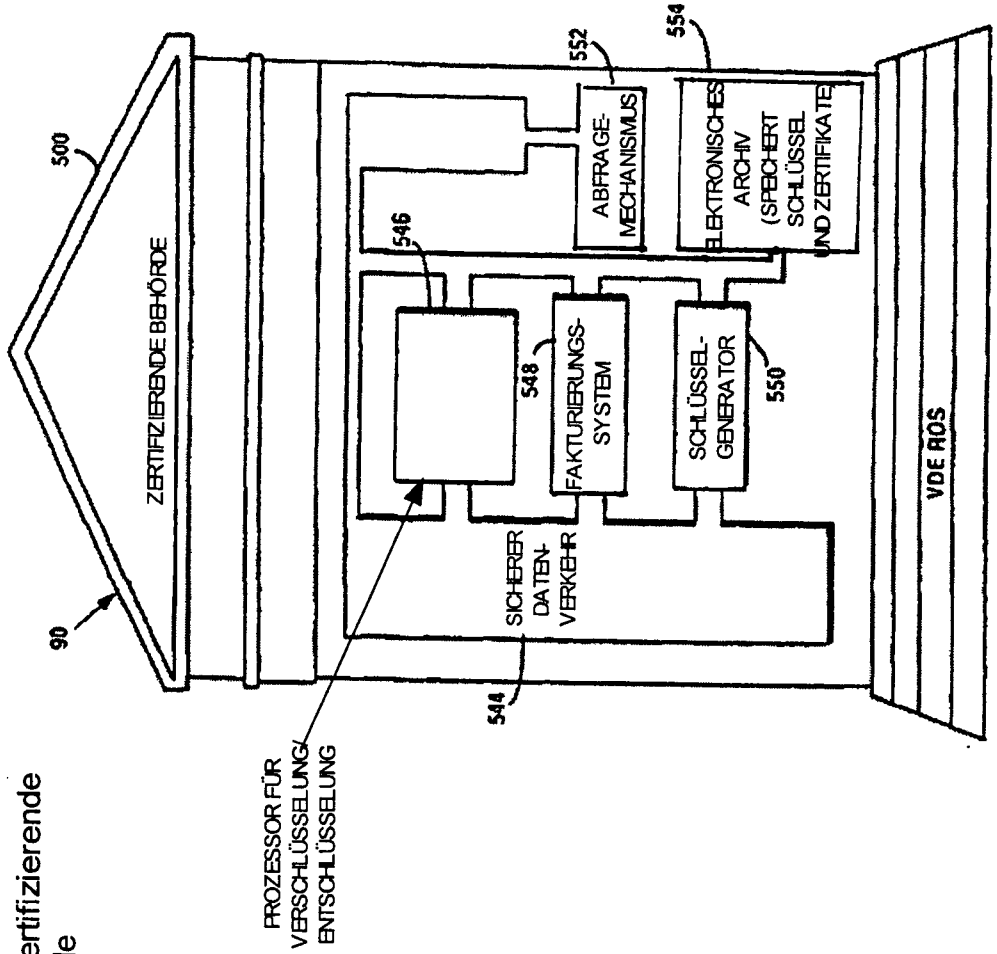


FIG. 48

Beispiel für eine zertifizierende Behörde

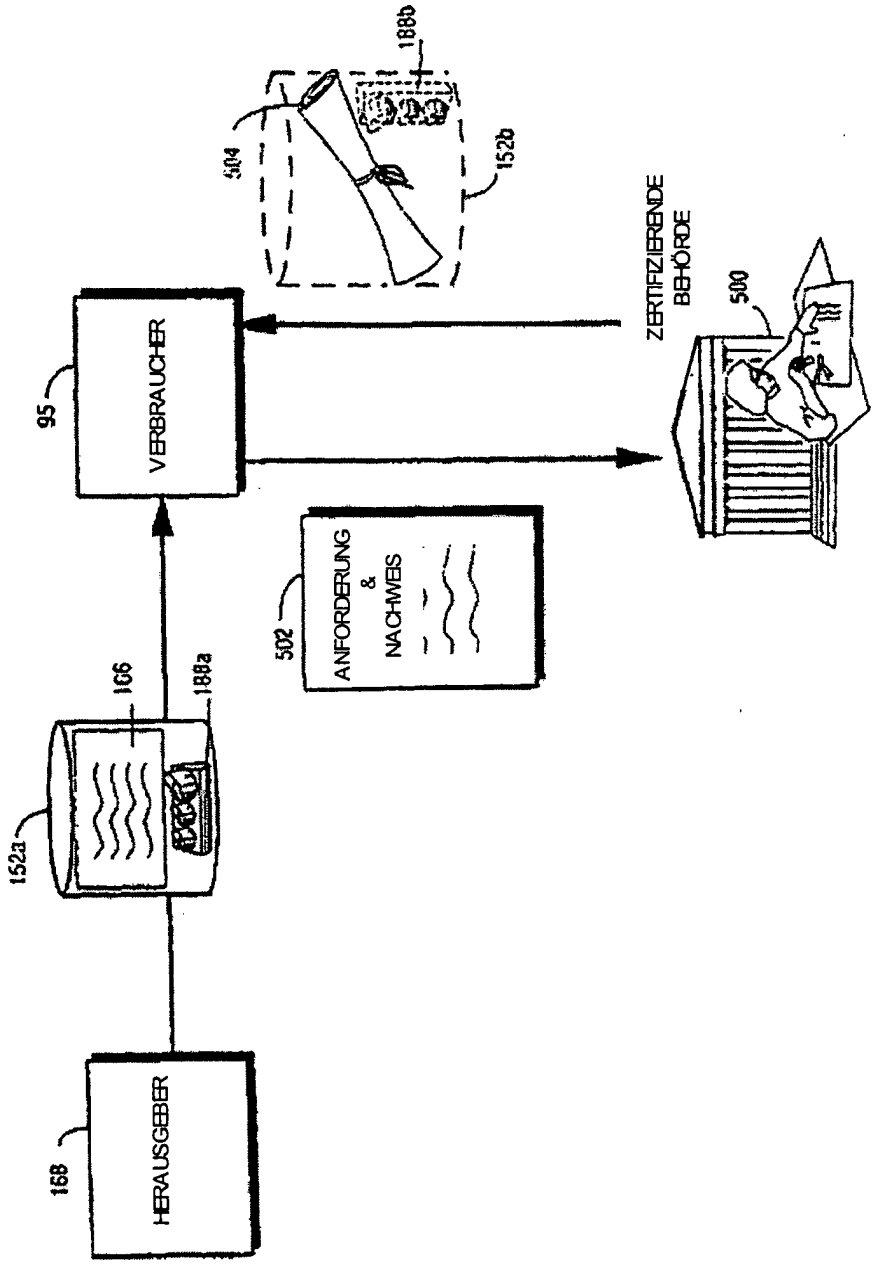


FIG. 49 BEISPIEL FÜR EINEN ZERTIFIZIERUNGSABLAUF

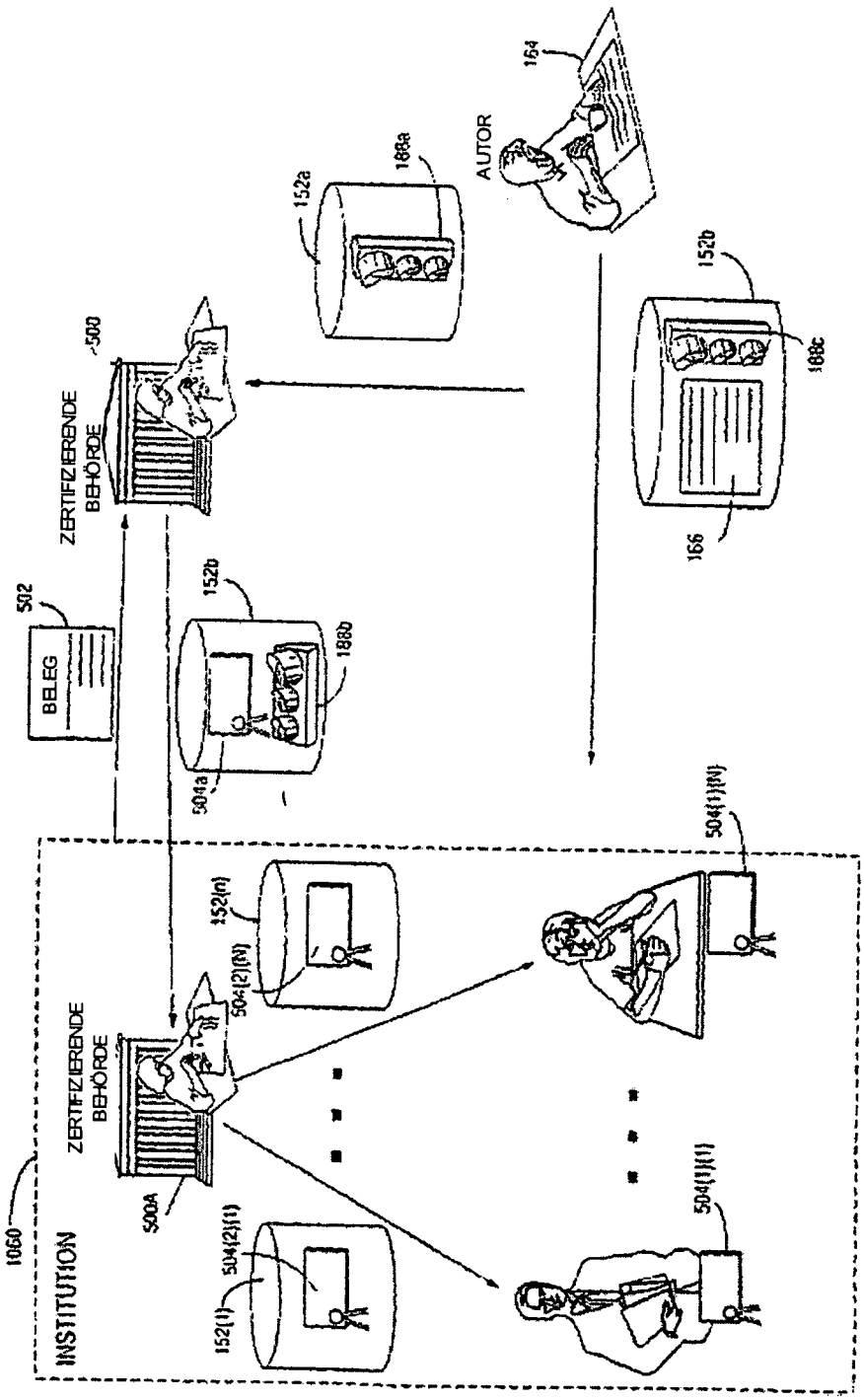
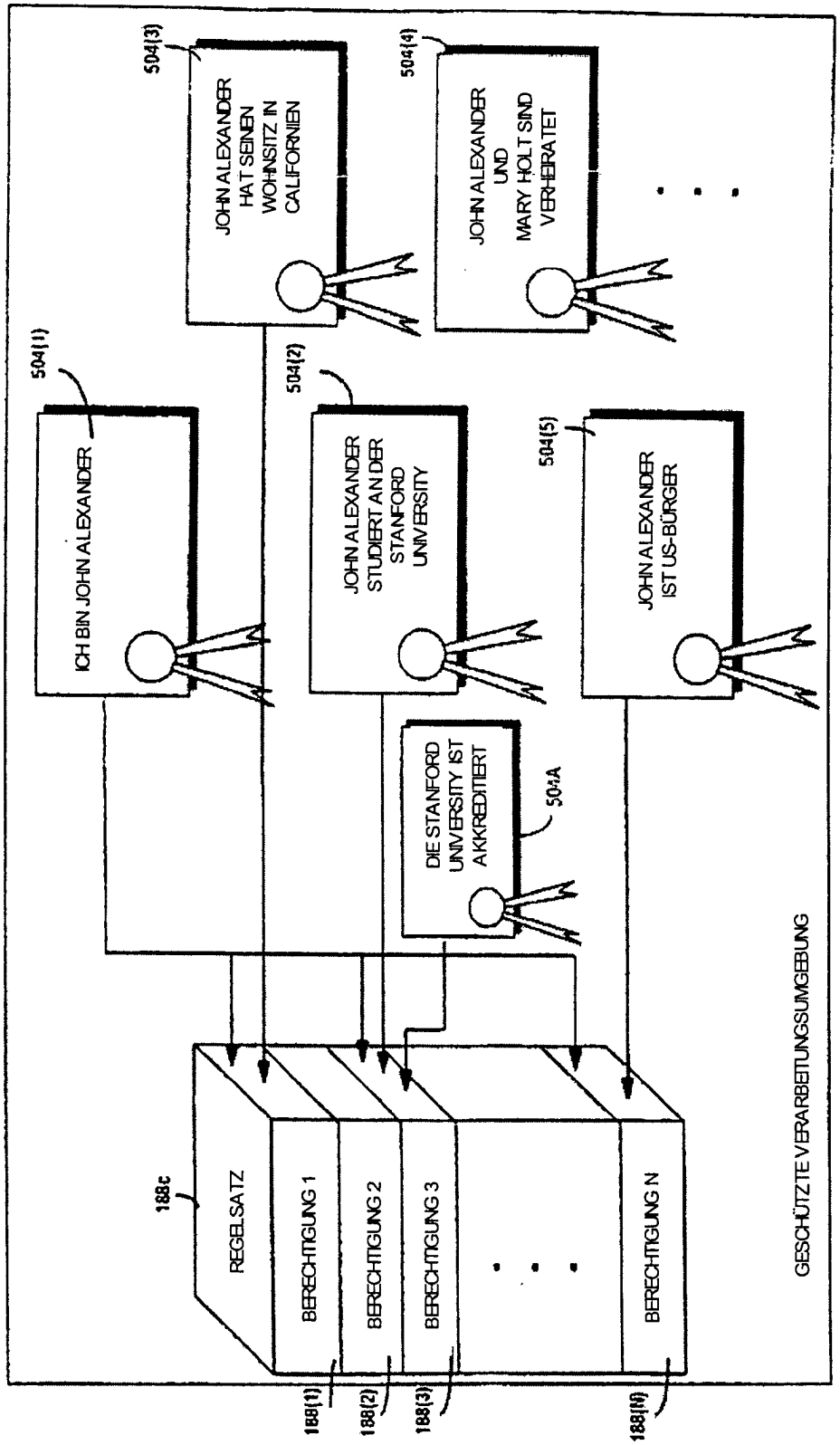


FIG. 50 VERTEILTE AUSTELLUNG VON ZERTIFIKATEN

FIG. 50A BEISPIEL FÜR EIN REGELSET UNTER VERWENDUNG VON ZERTIFIKATEN



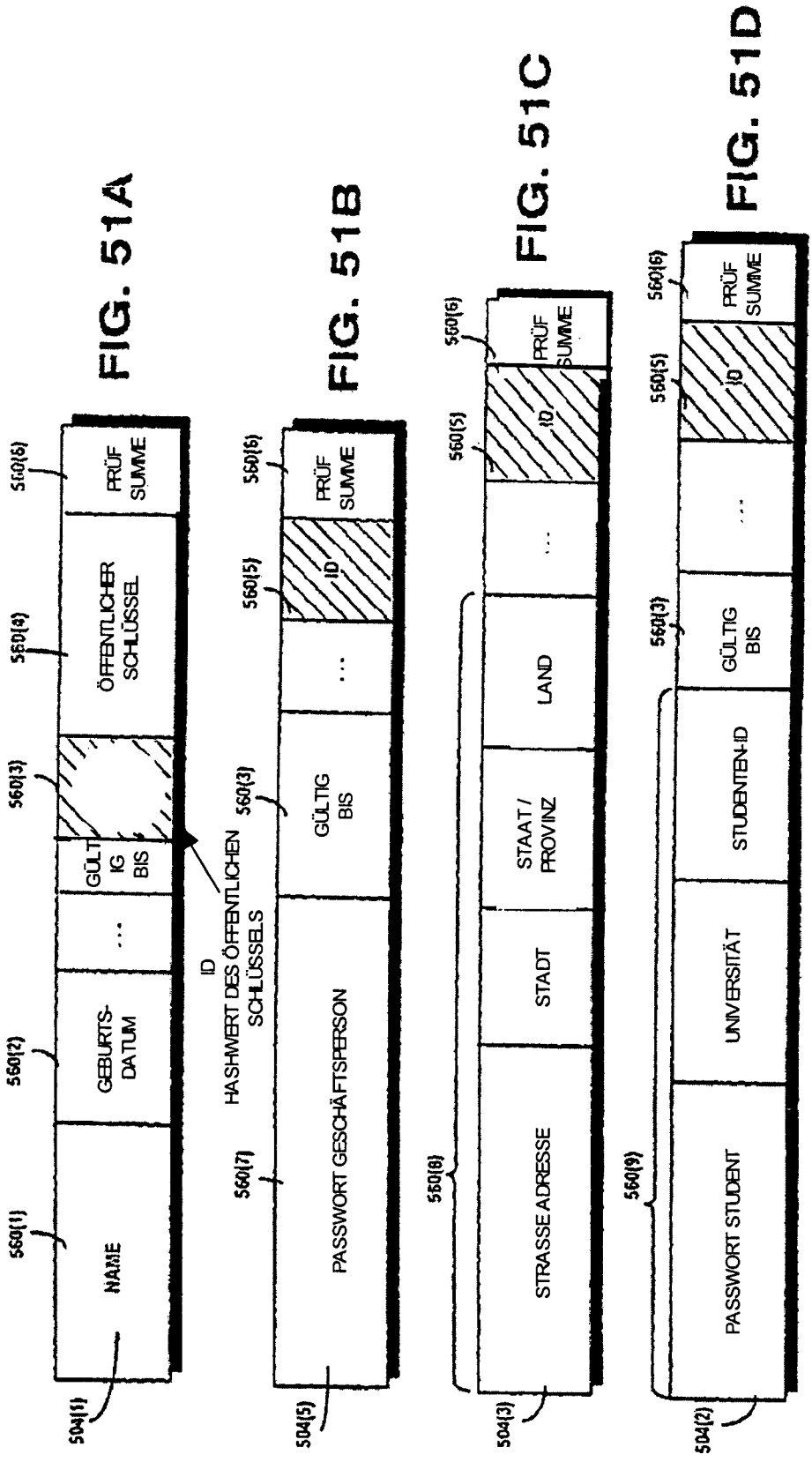


FIG. 51A

FIG. 51B

FIG. 51C

FIG. 51D

BEISPIELE FÜR DIGITALE ZERTIFIKATE

FIG. 51E ERZEUGUNG VON ZERTIFIKATEN AUF GRUNDLAGE ANDERER ZERTIFIKATE

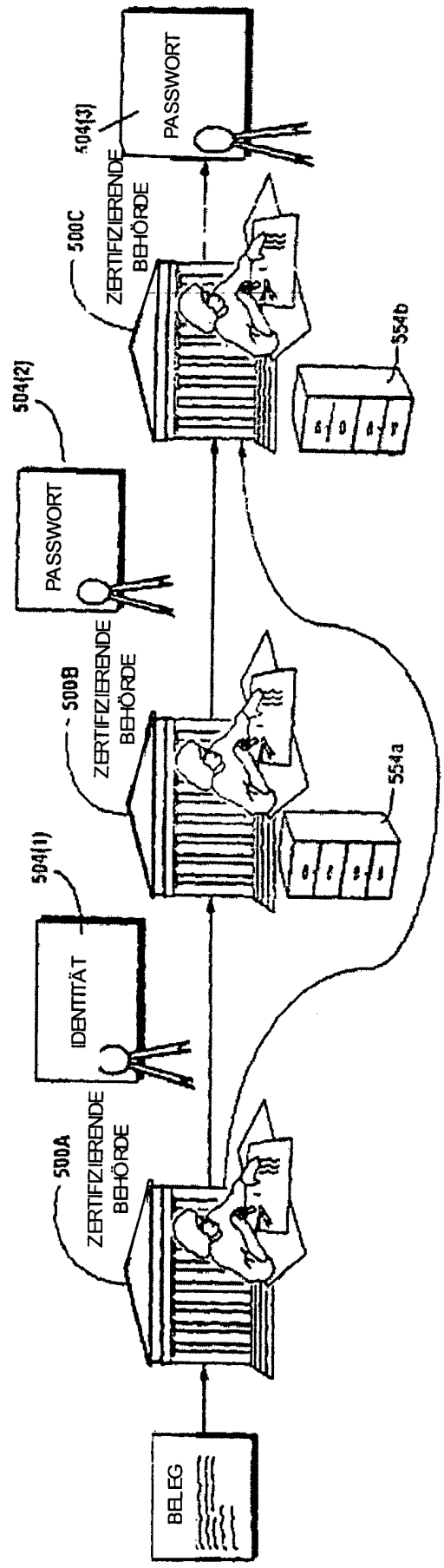


FIG. 51F

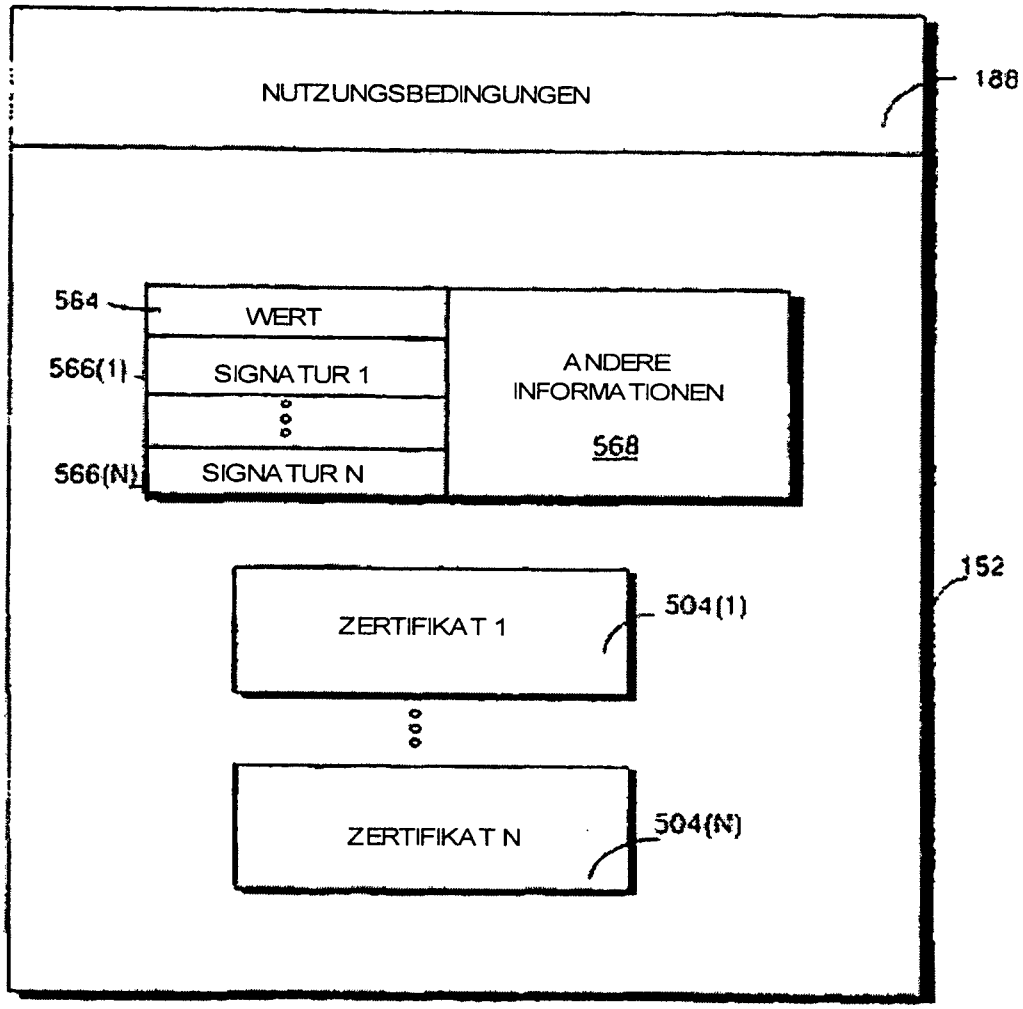

NUTZUNGSBEDINGUNGEN
188
564
WERT
566(1)
SIGNATUR 1
566(N)
SIGNATUR N
ANDERE INFORMATIONEN
568
152
ZERTIFIKAT 1
504(1)
ZERTIFIKAT N
504(N)

FIG. 51G

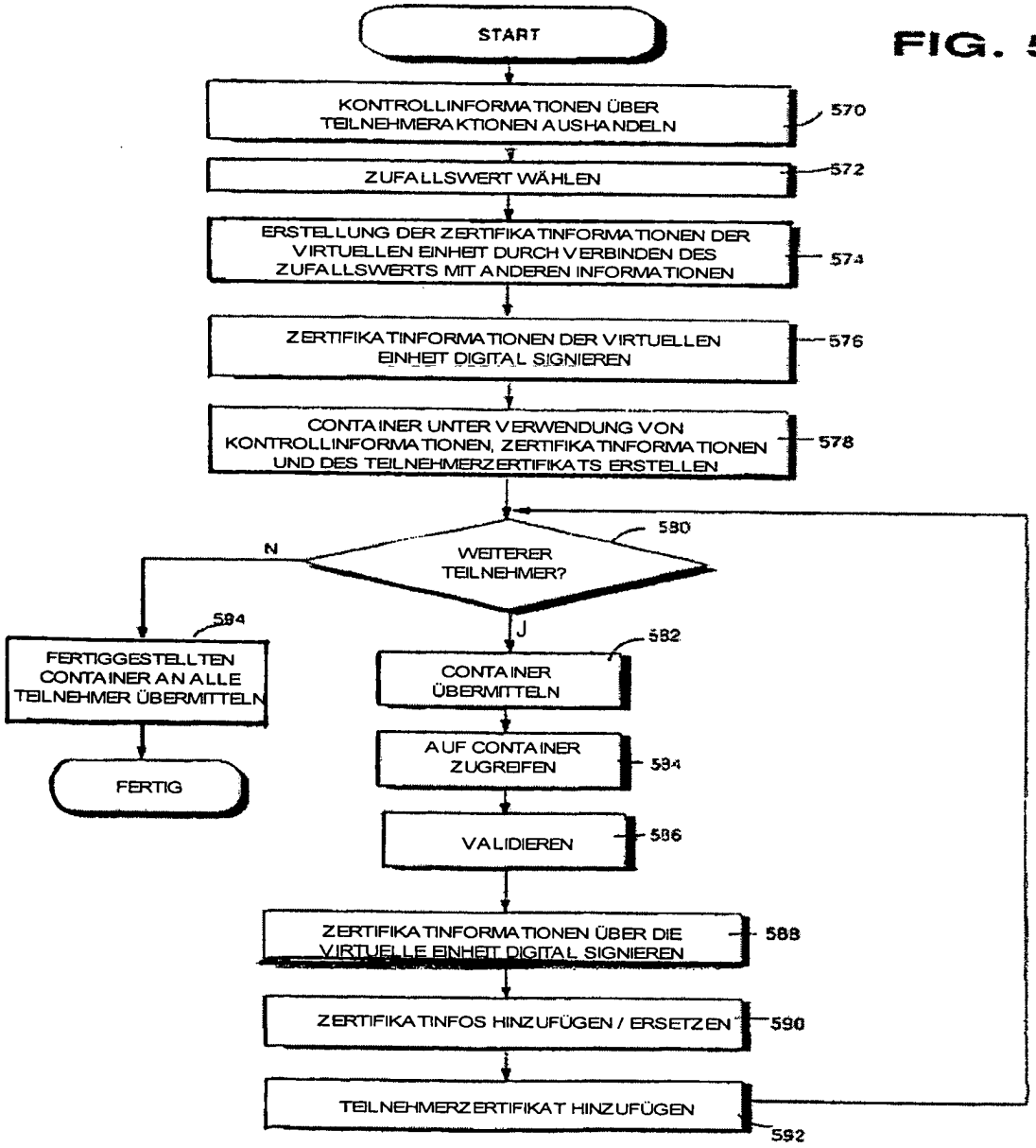
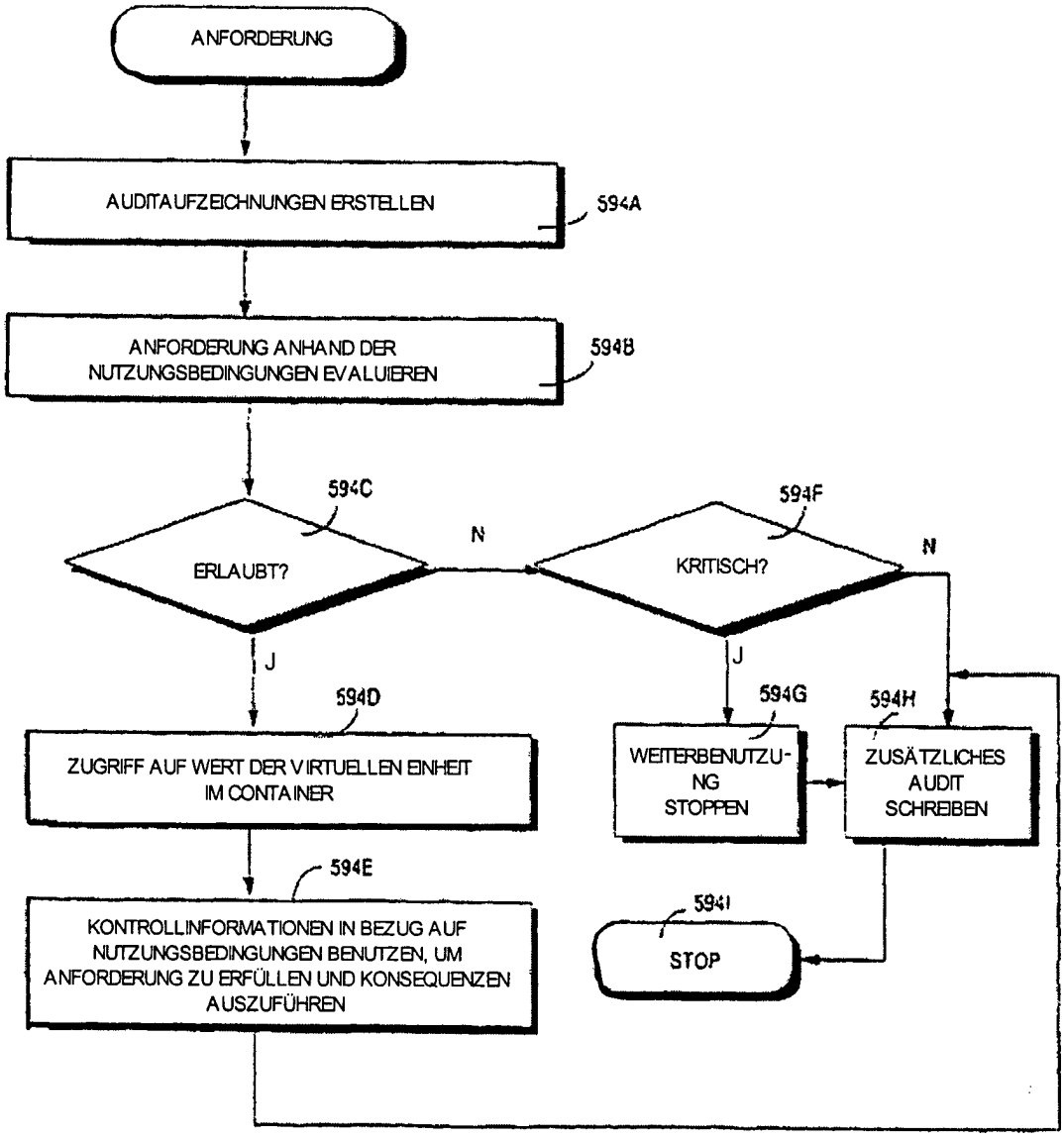

START
KONTROLLINFORMATIONEN ÜBER TEILNEHMERAKTIONEN AUSHANDELN
570
ZUFALLSWERT WÄHLEN
572
ERSTELLUNG DER ZERTIFIKATINFORMATIONEN DER VIRTUELLEN EINHEIT DURCH VERBINDEN DES ZUFALLSWERTS MIT ANDEREN INFORMATIONEN
574
ZERTIFIKATINFORMATIONEN DER VIRTUELLEN EINHEIT DIGITAL SIGNIEREN
576
CONTAINER UNTER VERWENDUNG VON KONTROLLINFORMATIONEN, ZERTIFIKATINFORMATIONEN UND DES TEILNEHMERZERTIFIKATS ERSTELLEN
578
WEITERER TEILNEHMER?
580
N
J
FERTIGGESTELLTEN CONTAINER AN ALLE TEILNEHMER ÜBERMITTELN
584
FERTIG
CONTAINER ÜBERMITTELN
582
AUF CONTAINER ZUGREIFEN
584
VALIDIEREN
586
ZERTIFIKATINFORMATIONEN ÜBER DIE VIRTUELLE EINHEIT DIGITAL SIGNIEREN
588
ZERTIFIKATINFOS HINZUFÜGEN / ERSETZEN
590
TEILNEHMERZERTIFIKAT HINZUFÜGEN
592

FIG. 51H


ANFORDERUNG
AUDITAUFZEICHNUNGEN ERSTELLEN
594A
ANFORDERUNG ANHAND DER NUTZUNGSBEDINGUNGEN EVALUIEREN
594B
594C
ERLAUBT?
N
594F
KRITISCH?
N
J
J
594D
ZUGRIFF AUF WERT DER VIRTUELLEN EINHEIT IM CONTAINER
594G
WEITERBENUTZUNG STOPPEN
594H
ZUSÄTZLICHES AUDIT SCHREIBEN
594E
KONTROLLINFORMATIONEN IN BEZUG AUF NUTZUNGSBEDINGUNGEN BENUTZEN, UM ANFORDERUNG ZU ERFÜLLEN UND KONSEQUENZEN AUSZUFÜHREN
594I
STOP

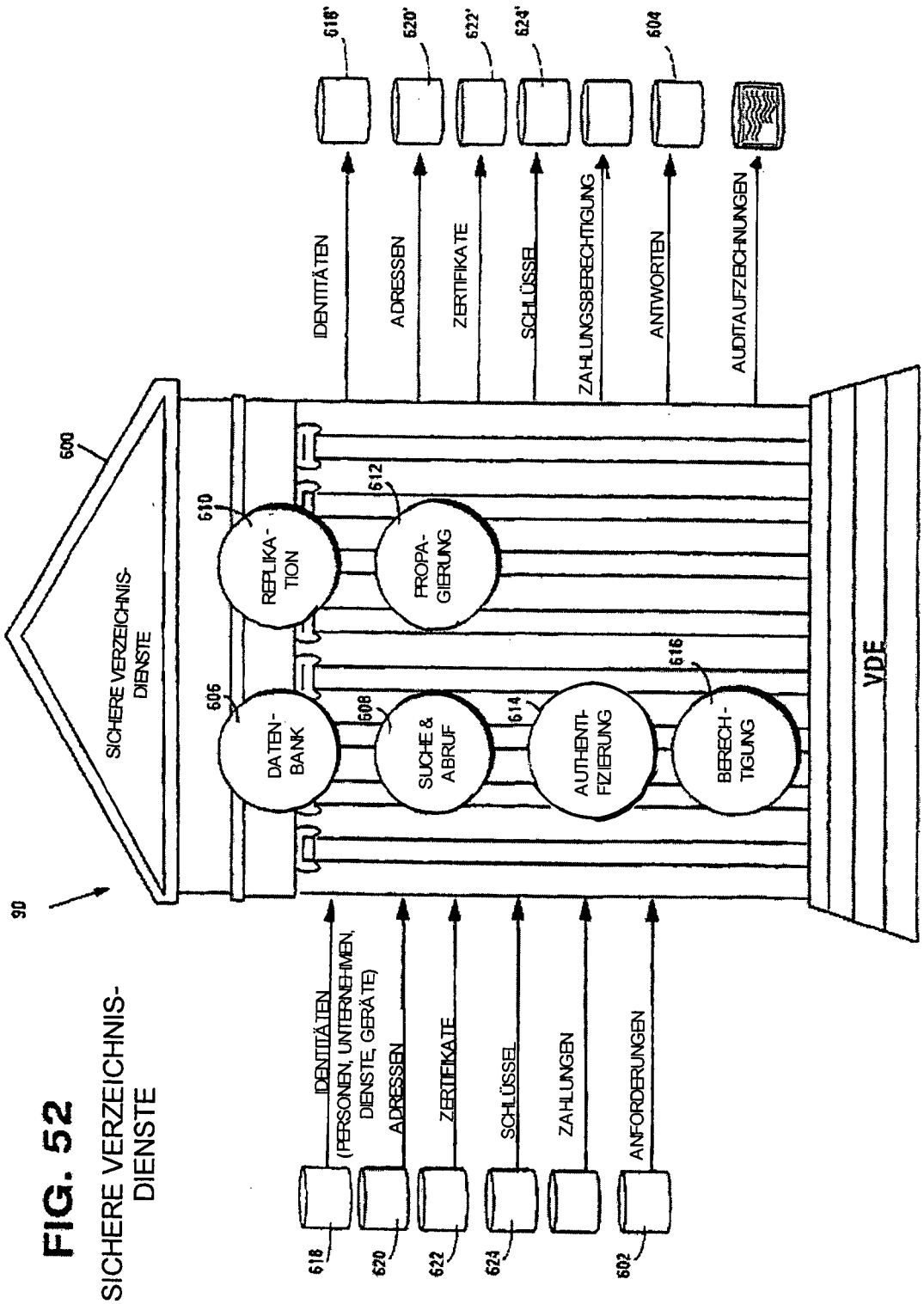


FIG. 52
SICHERE VERZEICHNIS-DIENSTE

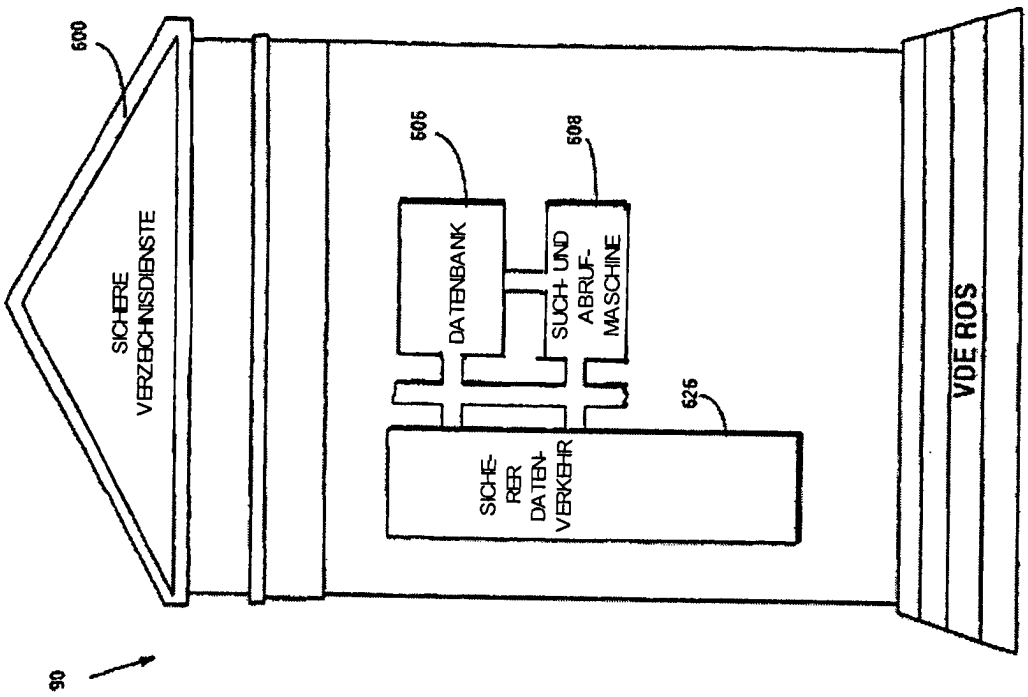


FIG. 53
BEISPIEL FÜR SICHERE VERZEICHNISDIENSTE

FIG. 54 BEISPIEL FÜR EINEN SICHEREN ABLAUF EINES VERZEICHNISDIENSTES

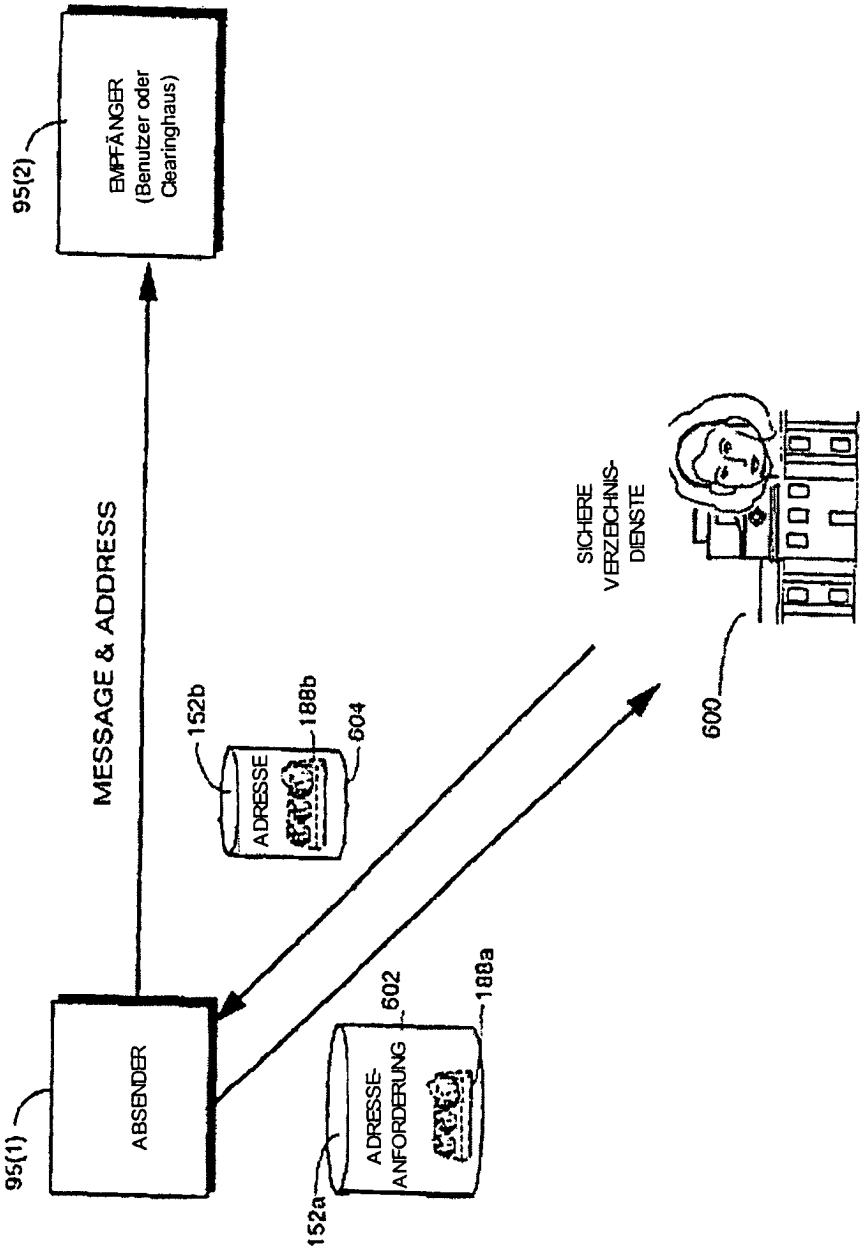


FIG. 55

BEISPIEL FÜR EINE TRANSAKTIONSBEHÖRDE

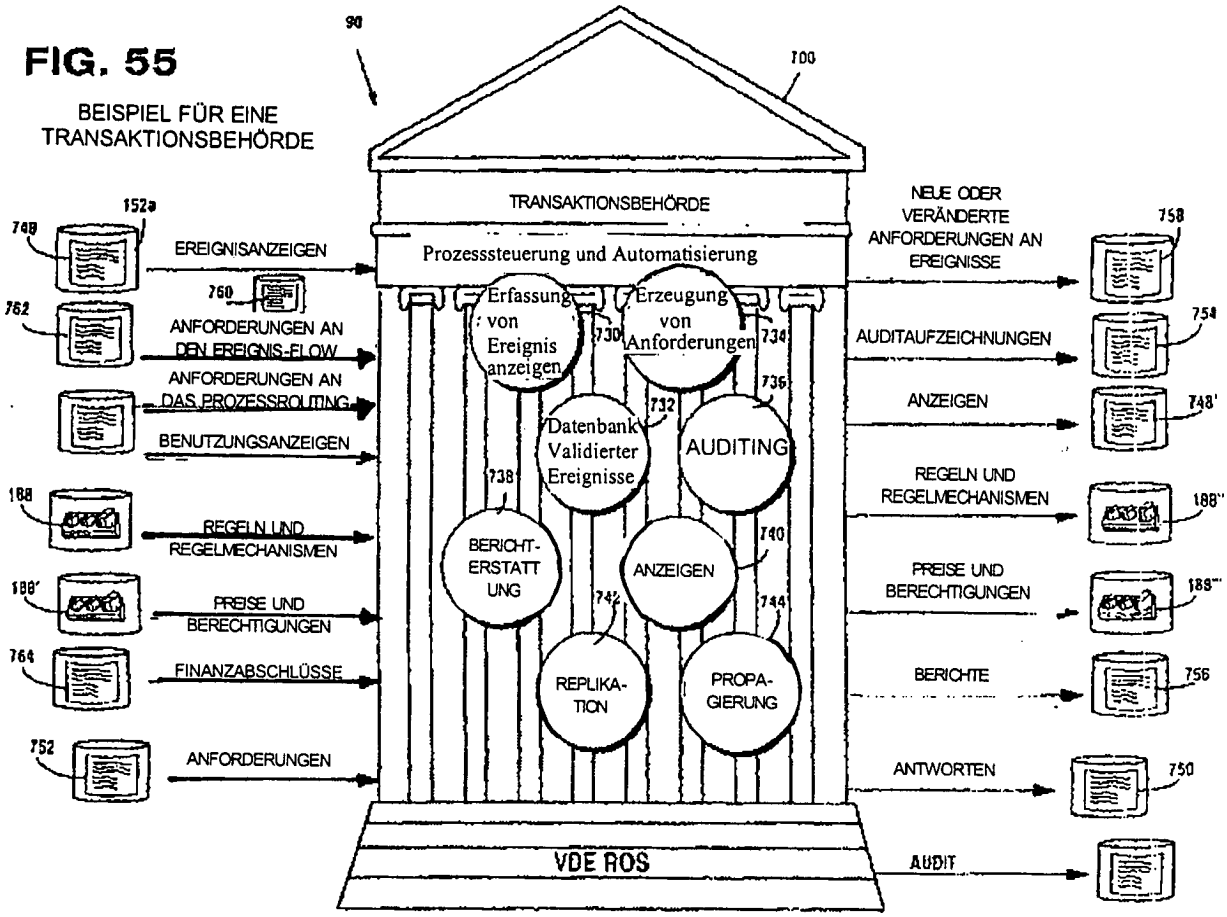
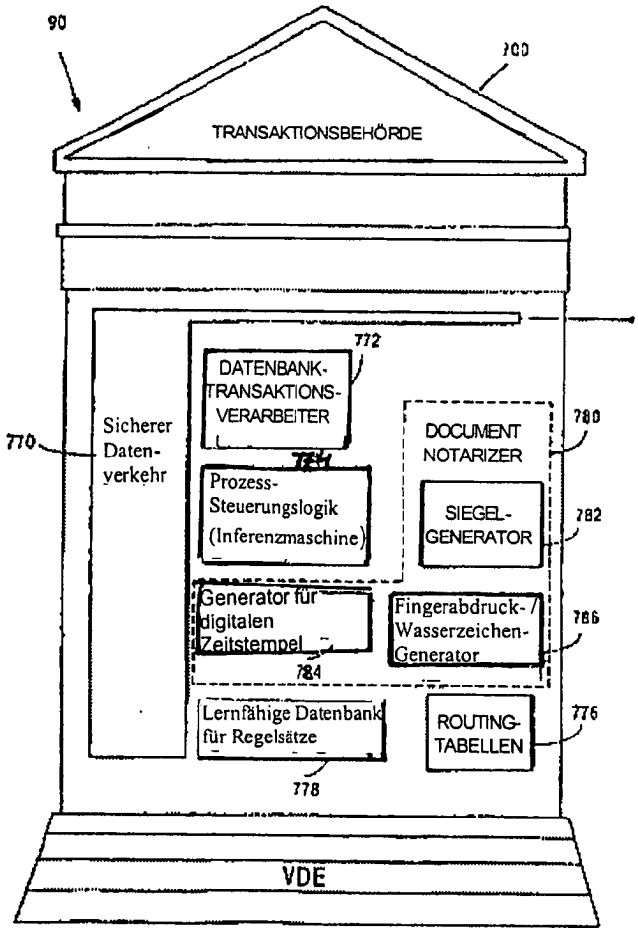


FIG. 56

BEISPIEL FÜR EINE TRANSAKTIONSBEHÖRDE



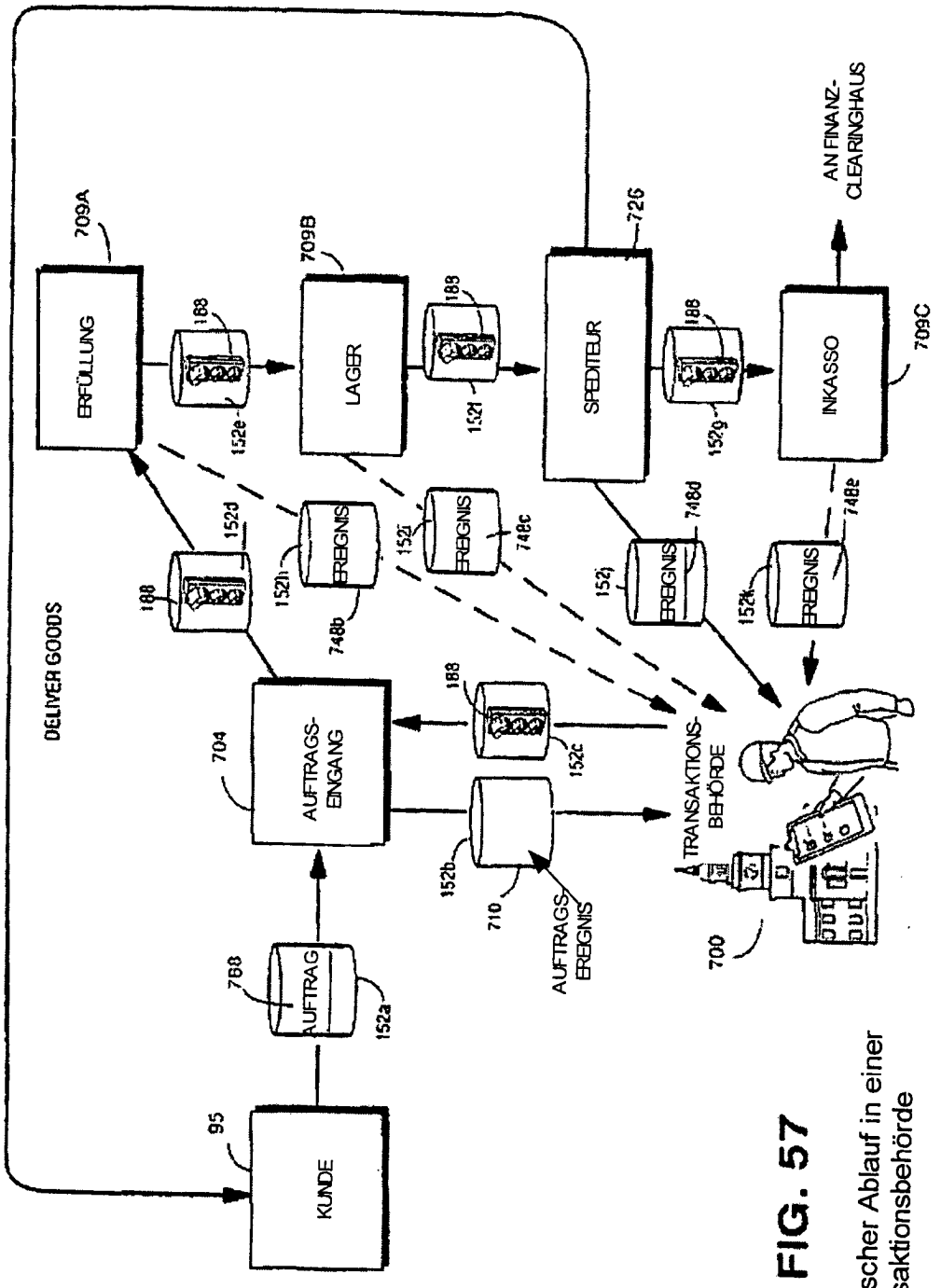


FIG. 57

Exemplarischer Ablauf in einer Transaktionsbehörde

Steuerung und Automatisierung

FIG. 58A

SCHAFFUNG EINES ÜBERGEORDNETEN REGELSATZES

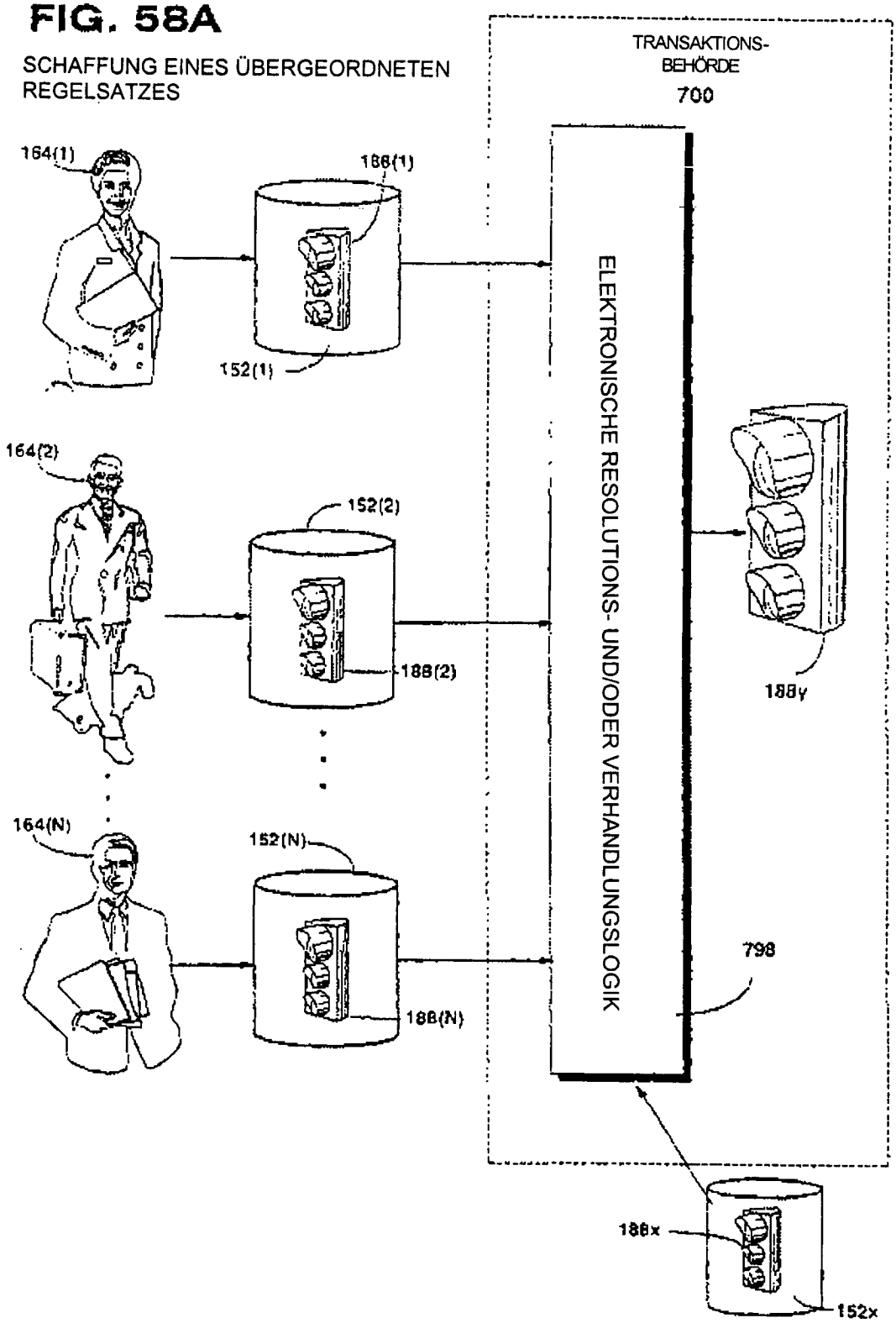
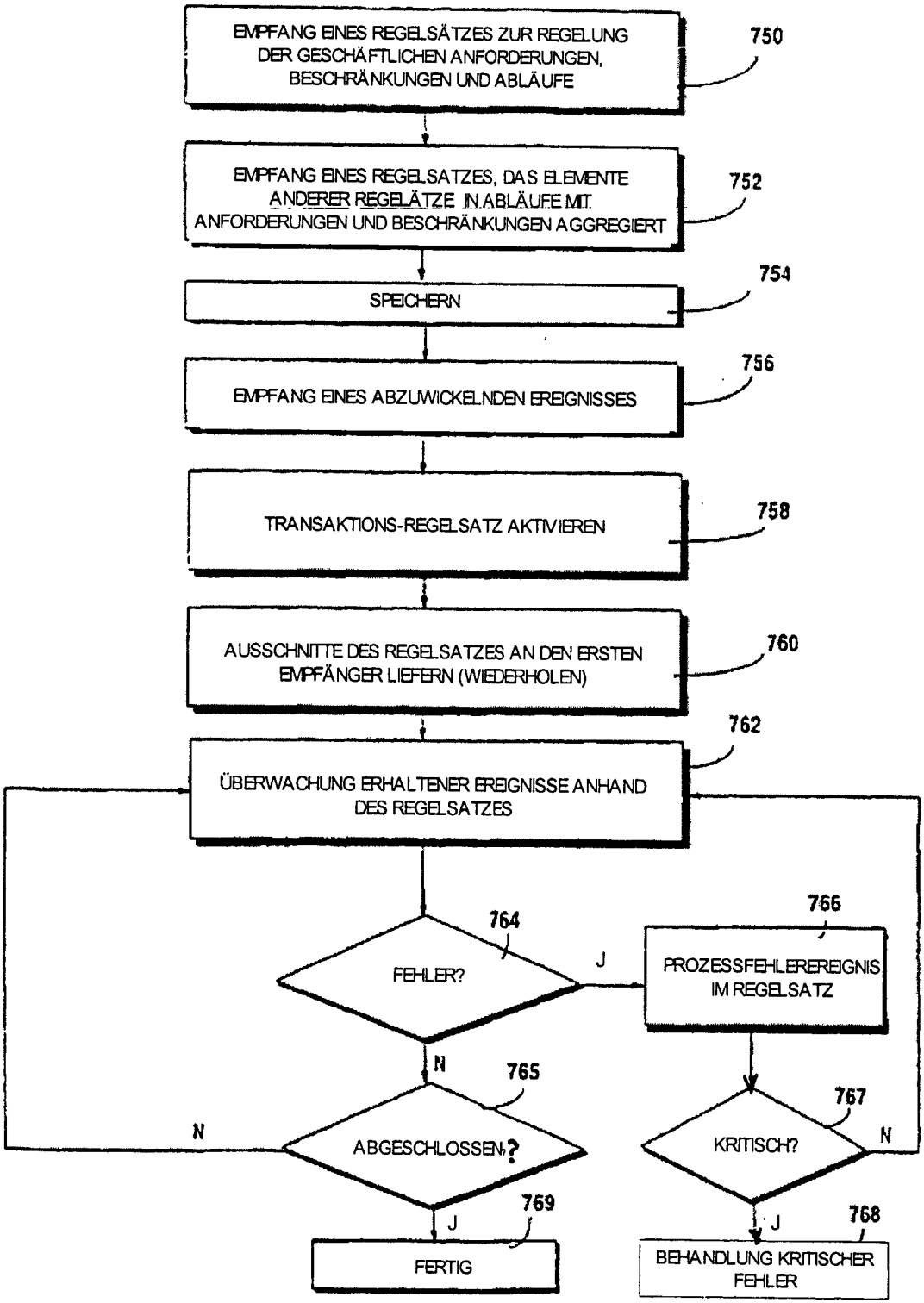


FIG. 58B BEISPIEL FÜR SCHRITTE EINER TRANSAKTIONSBEHÖRDE



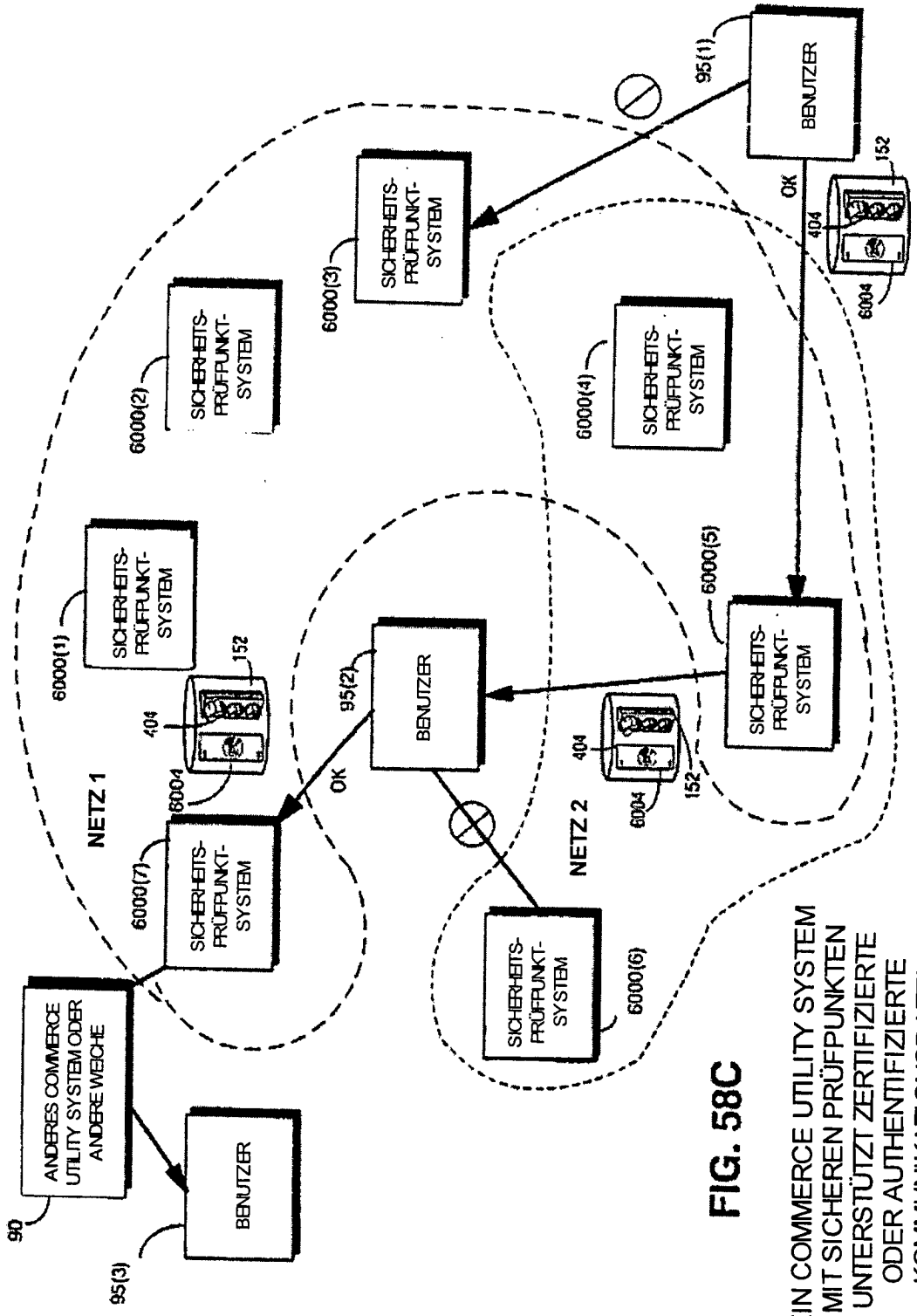
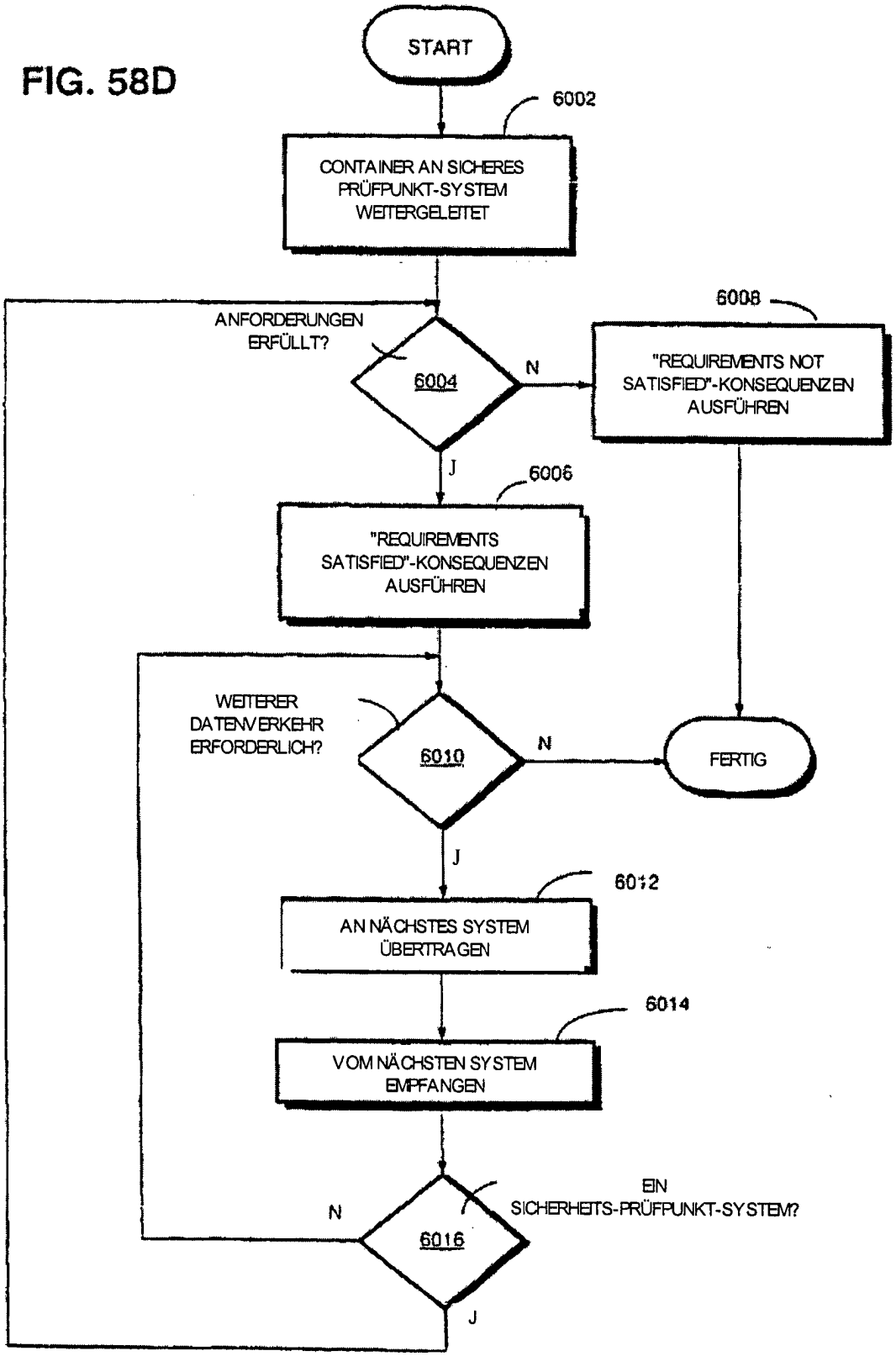


FIG. 58C

EIN COMMERCE UTILITY SYSTEM MIT SICHEREN PRÜFPUNKTEN UNTERSTÜTZT ZERTIFIZIERTE ODER AUTHENTIFIZIERTE KOMMUNIKATIONSDATEN

FIG. 58D


START
6002
CONTAINER AN SICHERES PRÜFPUNKT-SYSTEM WEITERGELEITET
ANFORDERUNGEN ERFÜLLT?
6004
N
6008
"REQUIREMENTS NOT SATISFIED"-KONSEQUENZEN AUSFÜHREN
J
6006
"REQUIREMENTS SATISFIED"-KONSEQUENZEN AUSFÜHREN
WEITERER DATENVERKEHR ERFORDERLICH?
6010
N
FERTIG
J
6012
AN NÄCHSTES SYSTEM ÜBERTRAGEN
6014
VOM NÄCHSTEN SYSTEM EMPFANGEN
EIN SICHERHEITS-PRÜFPUNKT-SYSTEM?
N
6016
J

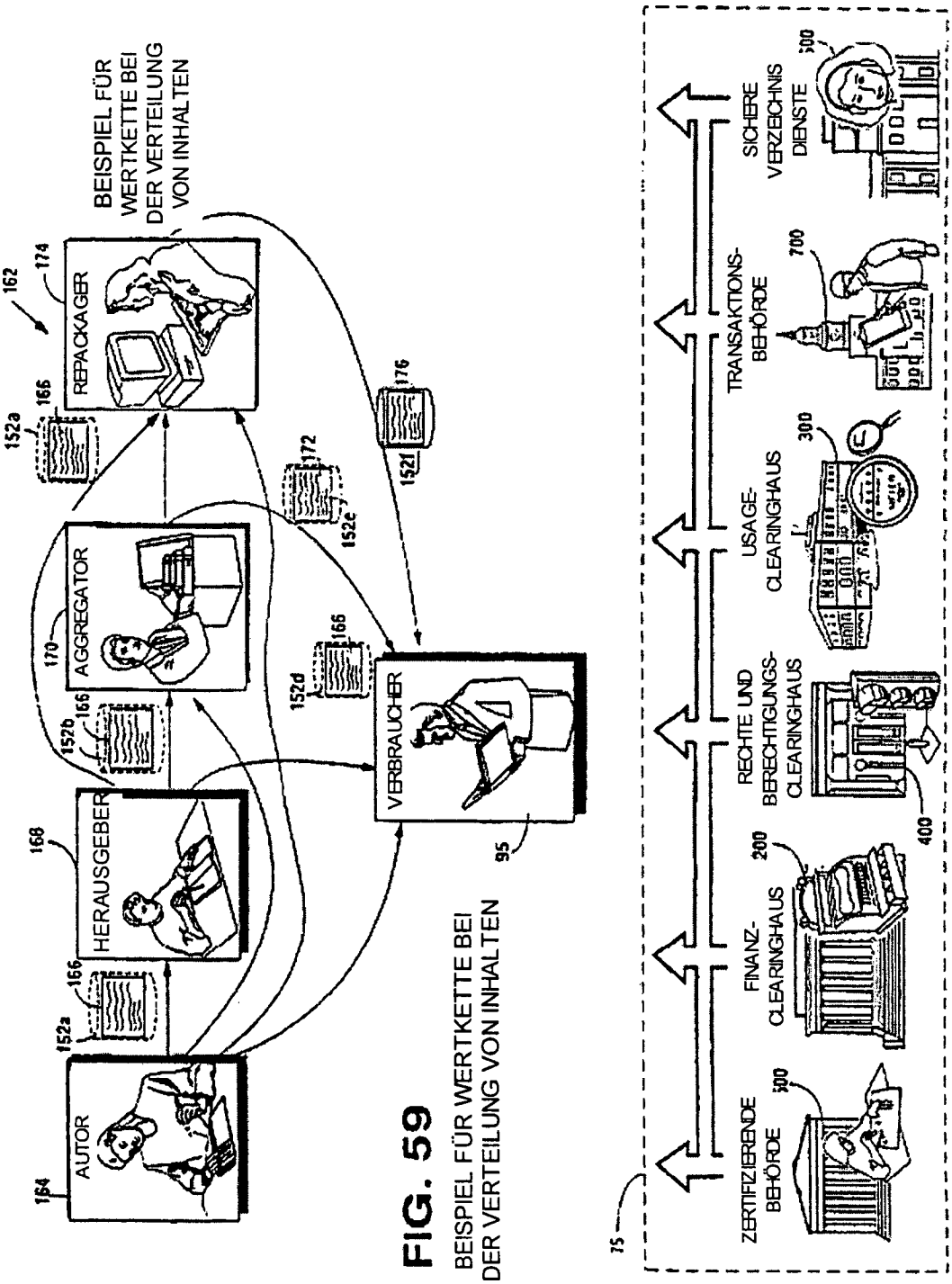


FIG. 59

BEISPIEL FÜR WERTKETTE BEI DER VERTEILUNG VON INHALTEN

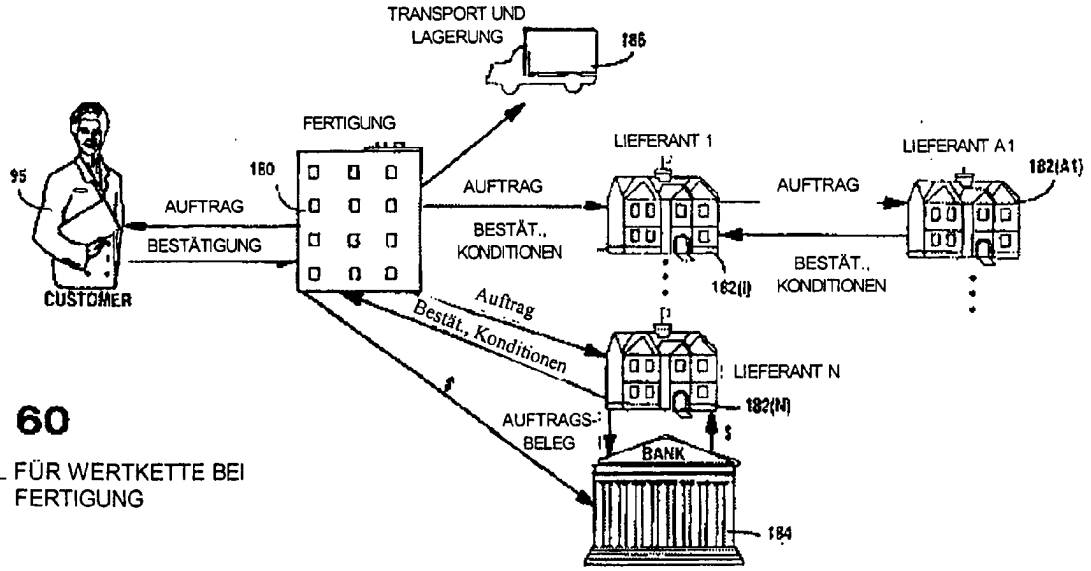
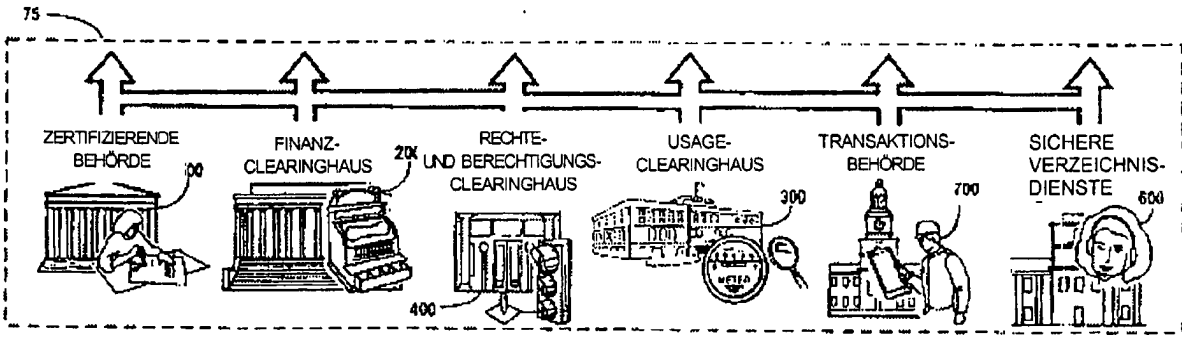


FIG. 60

BEISPIEL FÜR WERTKETTE BEI FERTIGUNG



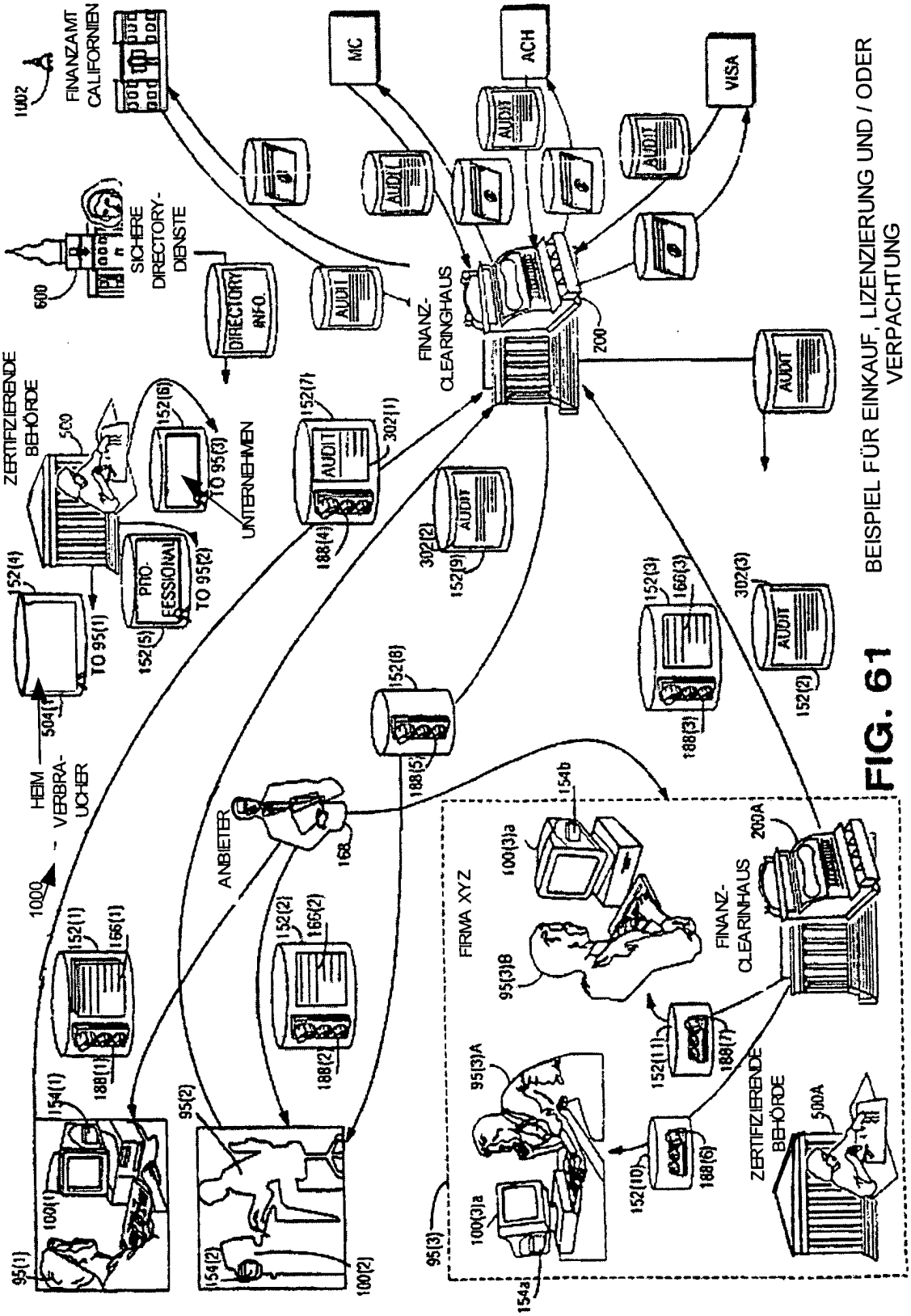


FIG. 61 BEISPIEL FÜR EINKAUF, LIZENZIERUNG UND / ODER VERPACHTUNG

FIG. 62

BEISPIEL FÜR EINKAUF UND BEZAHLUNG EINES MATERIELLEN ARTIKELS

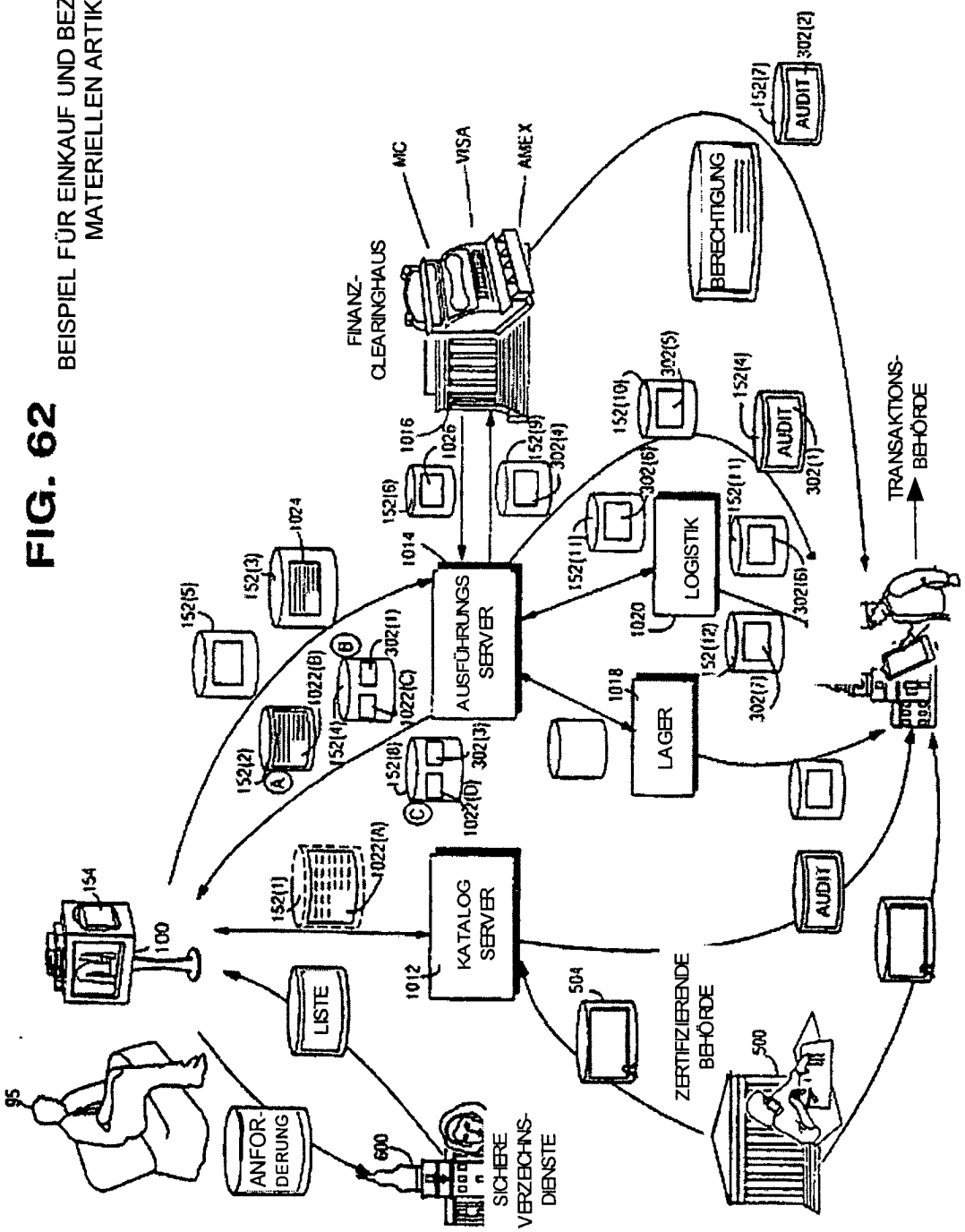


FIG. 63 BEISPIEL: KUNDE BEZAHLT AUF SICHEREM WEGE LEISTUNGEN

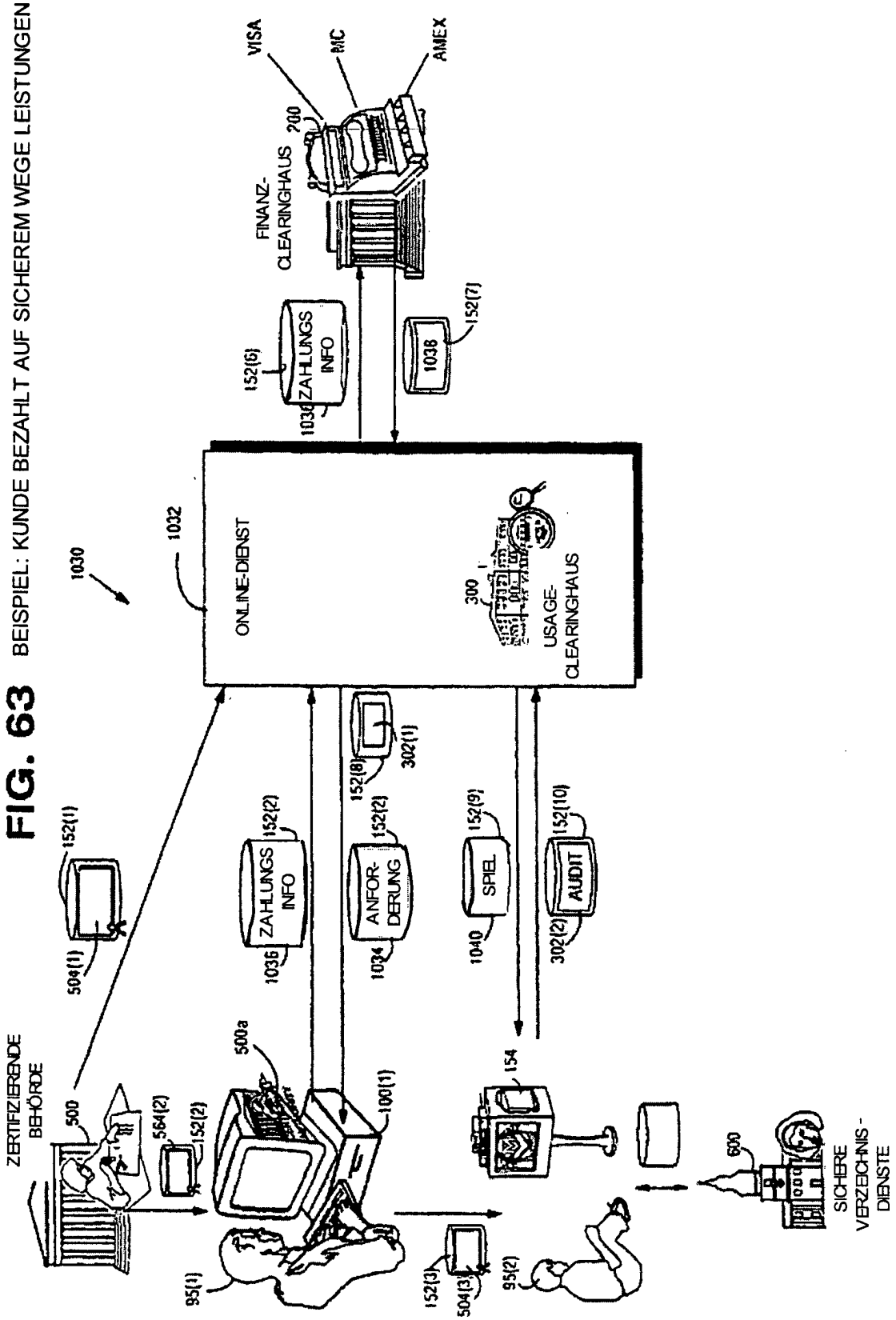
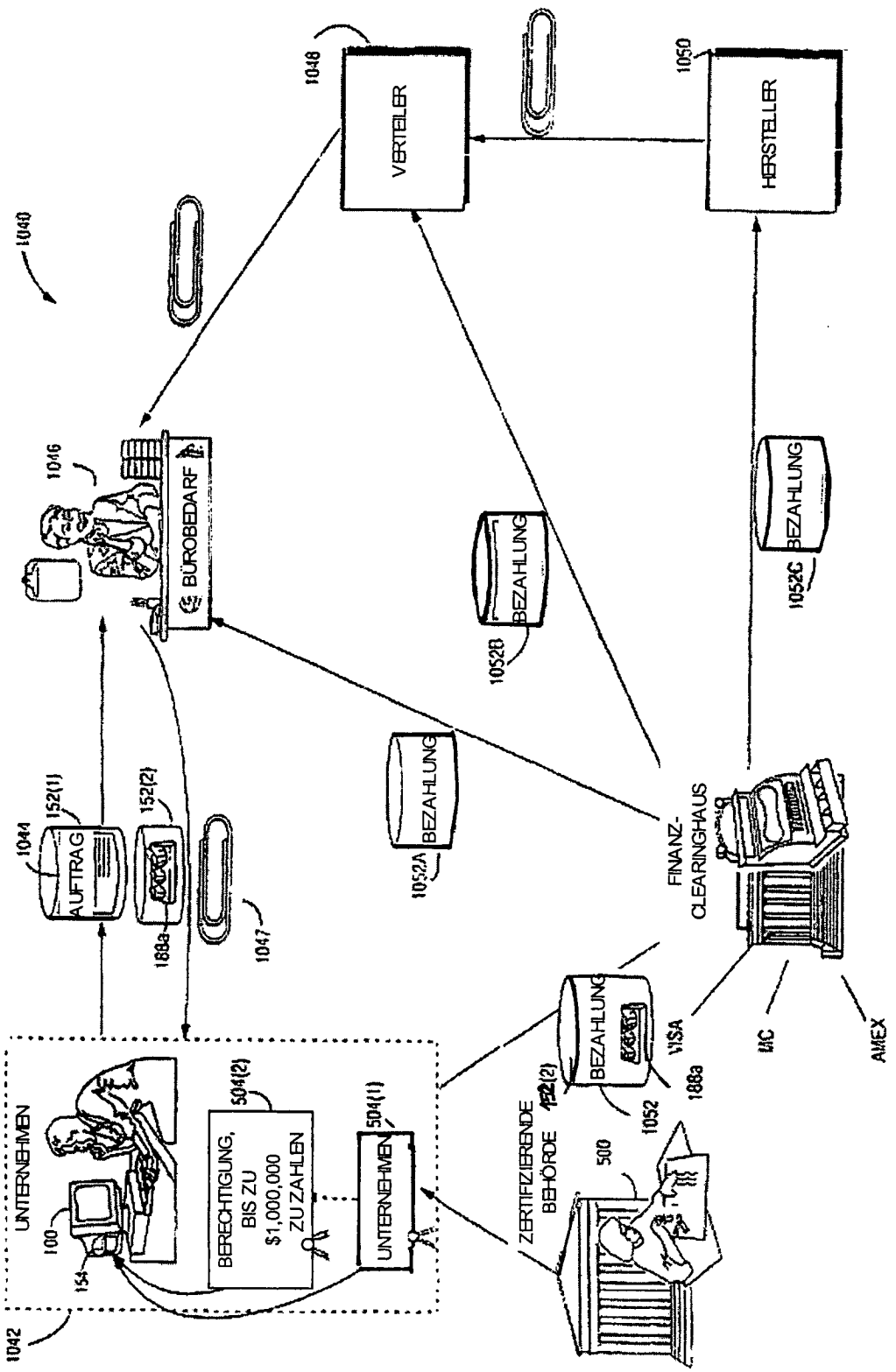


FIG. 64 BEISPIEL FÜR DIE DISAGGREGATION EINER WERTKETTE FÜR DEN EINKAUF MATERIELLER GÜTER



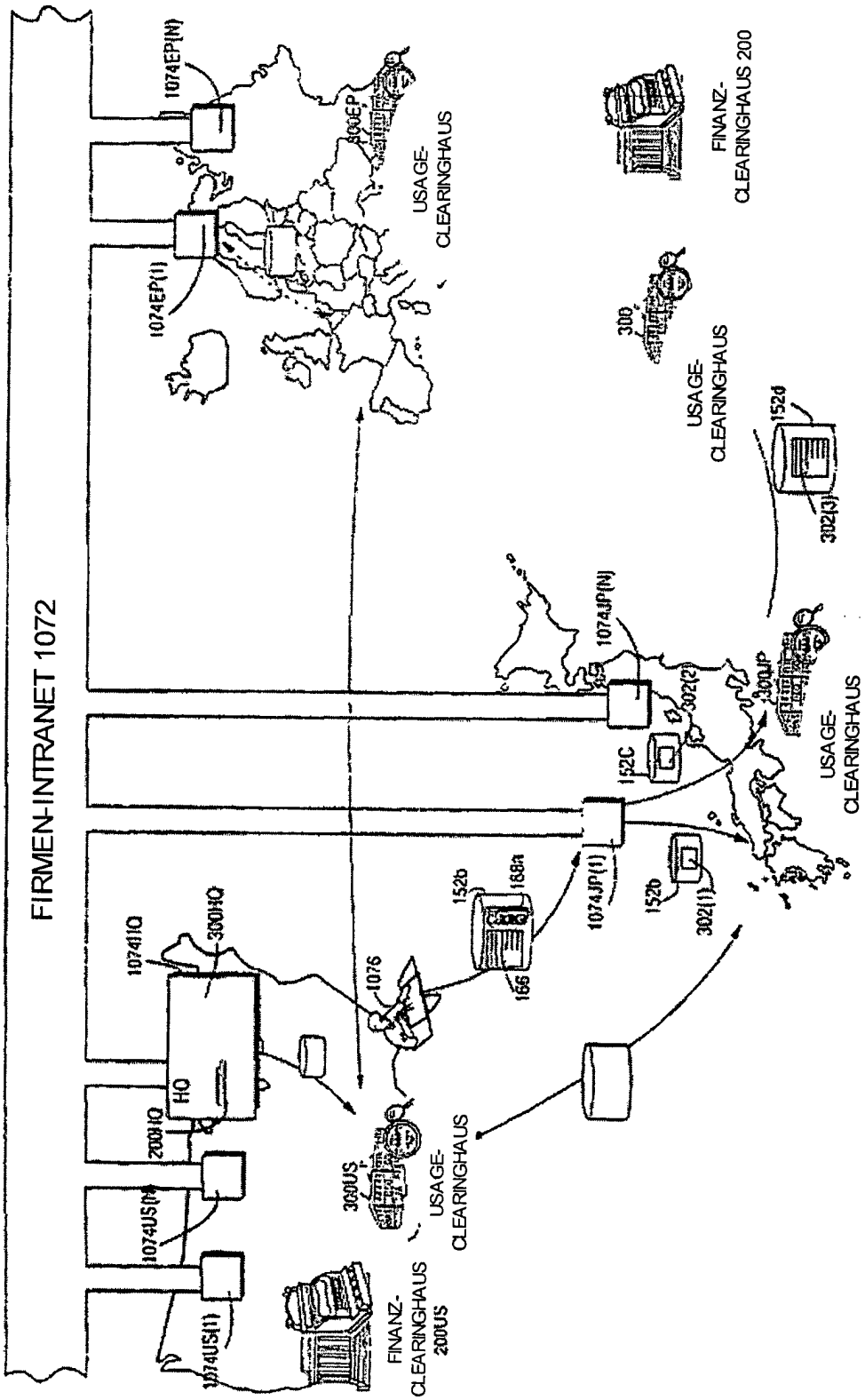


FIG. 65 KOOPERATION ZWISCHEN COMMERCE UTILITY SYSTEMS INNERHALB UND AUßERHALB EINES UNTERNEHMENS

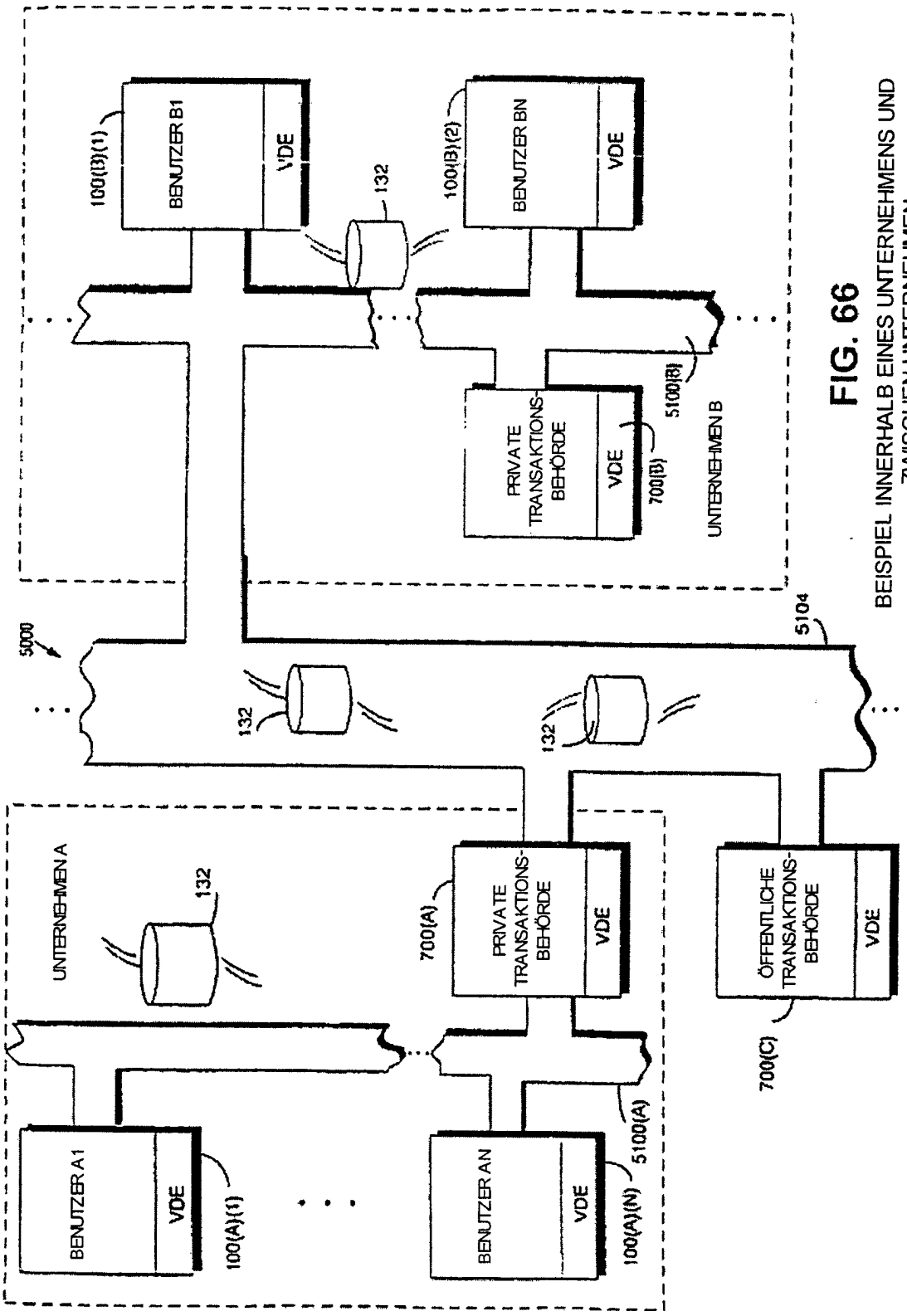


FIG. 66

BEISPIEL INNERHALB EINES UNTERNEHMENS UND ZWISCHEN UNTERNEHMEN

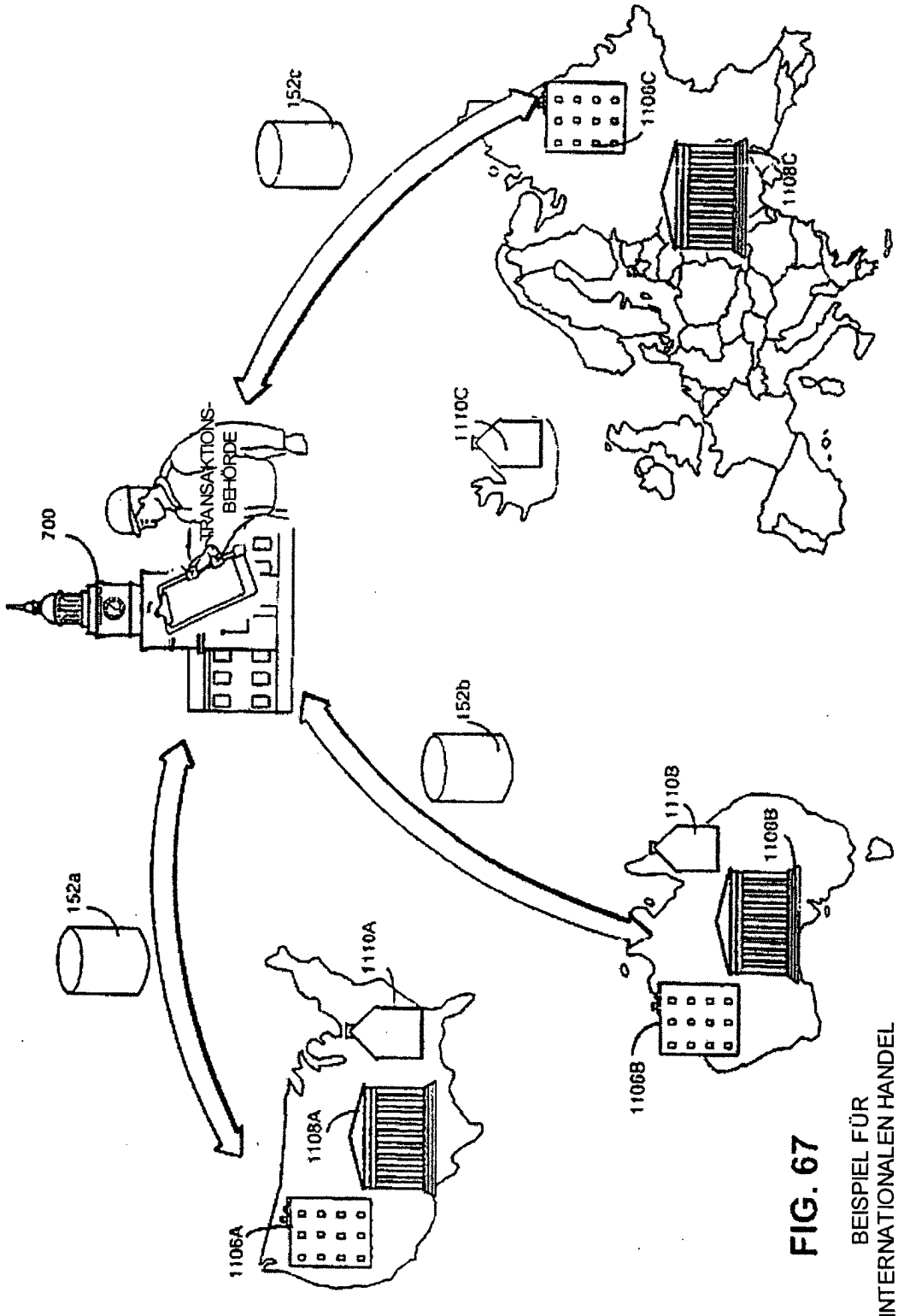


FIG. 67
BEISPIEL FÜR
INTERNATIONALEN HANDEL